PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-106148

(43)Date of publication of application : 24.04.1998

---

(51)Int.Cl. G11B 20/10

G06F 12/14

G09C 1/00

H04L 9/08

---

(21)Application number : 09-136709 (71)Applicant : TOSHIBA CORP

(22)Date of filing : 27.05.1997 (72)Inventor : KATO TAKEHISA

ENDO NAOKI

UNNO HIROAKI

KOJIMA TADASHI

HIRAYAMA KOICHI

---

(30)Priority

Priority number : 08170399

Priority date : 28.06.1996

Priority country : JP

---

(54) CIPHERING METHOD, DECODING METHOD, RECORDING AND REPRODUCING DEVICE, DECODING DEVICE, DECODING UNIT DEVICE, RECORDING MEDIUM, MANUFACTURE OF RECORDING MEDIUM AND METHOD OF MANAGING KEY

(57)Abstract:

PROBLEM TO BE SOLVED: To protect a copyright from piracy in preventing illegal copies by ciphering a data with a 1st key and ciphering this 1st key with predetermined plural 2nd keys.

SOLUTION: A 2nd session key Sk' is generated by a session key generating circuit 111, and is decoded by a decoding circuit 112 with a master key Mk and then ciphered by a ciphering circuit 104 with the key Mk, so that the key Sk' generated by the circuit 111 is obtained. Then, a 1st session key ciphered by the key Mk recorded on a DVD 101 is ciphered by the key Sk' and is sent to the circuit 112, where this key is decoded by the key Mk to obtain the 1st session key Mk. Then, a data ciphered by a key Sk recorded on the DVD 101 is read out, and is processed by a demodulation/ error correction circuit 118, and afterward, the received data is decoded by the circuit 112 with the key Sk to obtain a plain styled data. Thus, the decoded data does not flow in a CPU.BUS 110, and for example, even when this data is stored in a storage medium, the data cannot be reproduced to be used. Consequently, an illegal act of making unauthorized copies is prevented to protect the copyright from piracy.

LEGAL STATUS [Date of request for examination] 16.12.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3093678

[Date of registration] 28.07.2000

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The encryption approach characterized by enciphering data with the 1st key and enciphering, respectively with two or more 2nd keys which were able to define said 1st key beforehand.

[Claim 2] The record medium characterized by recording at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively.

[Claim 3] The manufacture approach of the record medium characterized by recording at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively in the same record medium.

[Claim 4] The information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively is inputted at least. The decode approach which can decode said 1st key using at least one of said the 2nd key, and is characterized by using this 1st key, and decoding and obtaining said data after judging by the predetermined approach that the 1st obtained key is a right thing.

[Claim 5] An input means to input at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively, Said 1st key is decoded and obtained based on the information inputted from said input means using at least one of said the 2nd key within a storage means to memorize at least one of said the 2nd key, and this storage means. Decode equipment characterized by having used this 1st key and having a decode means to decode and obtain said data after judging by the predetermined approach that the 1st obtained key is a right thing.

[Claim 6] The read-out means which reads these information from the record medium which memorized at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively at least, Said 1st key is decoded and obtained based on the information read from said read-out means using at least one of said the 2nd key within a storage means to memorize at least one of said the 2nd key, and this storage means. The record regenerative apparatus characterized by having used this 1st key and having a decode means to decode and obtain said data after judging by the predetermined approach that the 1st obtained key is a right thing.

[Claim 7] Two or more 2nd keys beforehand set to the 1st manager are made to

keep it at least. The management method of the key characterized by making the 2nd manager manage at least the information which enciphered data with the 1st key, and the information which enciphered said 1st key with said two or more 2nd keys defined beforehand, respectively, and making the 3rd manager manage at least one of said the 2nd key.

[Claim 8] The read-out means which reads these information from the record medium which memorized at least the 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging at least, One is used. it chose according to the sequence defined [from] among said 2nd key memorized by a storage means to memorize at least one of said the 2nd key, and said storage means -- While decoding the 1st one enciphered key which was chosen [from] according to the defined sequence among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing.. Decode equipment characterized by having the 1st decode means which repeats said selection and said judgment until the 1st key judged to be a right thing is obtained, and the 2nd decode means which decodes and obtains said data using said 1st key obtained as a right thing by this 1st decode means.

[Claim 9] The 2nd information which enciphered, respectively and was acquired from the record medium with two or more 2nd keys which were able to define beforehand the 1st information which was read at least, and which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging It tells the 2nd unit through the CPU bus of a calculating machine from the 1st unit connected to the driving gear of said record medium, without minding the CPU bus of a calculating machine or it was built in the driving gear of said record medium. It is decode equipment which decodes said data at least in said 2nd unit. Said 1st unit While telling said 1st, 2nd, and 3rd information to said 2nd unit through the CPU bus of said calculating machine, at least about said 2nd and 3rd information It has a means for telling insurance, without being acquired from the exterior. Said 2nd unit While receiving said 1st, 2nd, and 3rd information from said 1st unit through the CPU bus of said calculating machine, at least about said 2nd and 3rd information The means for receiving safely, without being acquired from the exterior, and a storage means to memorize at least one of said the 2nd key, While decoding the 1st one enciphered key which was chosen according to the sequence which was chosen according to the sequence defined [from] among said 2nd key memorized by said storage means, and which used one and was defined [from] among said 2nd information It judges whether this 1st key obtained by said decode based on

this decode result and said 3rd information at least is a right thing. Decode equipment characterized by having the 1st decode means which repeats said selection and said judgment until the 1st key judged to be a right thing is obtained, and the 2nd decode means which decodes and obtains said data using said 1st key obtained as a right thing by this 1st decode means.
 [Claim 10] The 1st information which enciphered the 3rd key with the 1st key and was acquired, and said 1st key are enciphered with two or more 2nd keys which were able to be defined beforehand, respectively. The read-out means which reads these information from the record medium which memorized the 4th information which enciphered the 2nd acquired information, the 3rd information used for a key judging, and data with said 3rd key, and was acquired at least at least, One is used. it chose according to the sequence defined [from] among said 2nd key memorized by a storage means to memorize at least one of said the 2nd key, and said storage means -- While decoding the 1st one enciphered key which was chosen [from] according to the defined sequence among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. The 1st decode means which repeats said selection and said judgment until the 1st key judged to be a right thing is obtained, Decode equipment characterized by having the 2nd decode means which decodes and obtains said 3rd key using

said 1st key obtained as a right thing by this 1st decode means, and the 3rd decode means which decodes and obtains said data using said 3rd key obtained by this 2nd decode means.

[Claim 11] Said 3rd information is the information which enciphered said 1st key for said 1st key itself, and was acquired. Said 1st decode means The key which decoded one of said 2nd information and was obtained using one of said the 2nd key memorized by said storage means, Decode equipment given in claim 8 characterized by being what judged as this key being the 1st key of the right when the key which decoded said said 3rd information and was obtained using this key is in agreement thru/or any 1 term of 10.

[Claim 12] Said data are decode equipment given in claim 8 characterized by being a thing containing at least one of key information, a document, voice, an image, and programs thru/or any 1 term of 11.

[Claim 13] These information is read from the record medium which memorized at least the 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging at least. While decoding the 1st one enciphered key which was chosen [from] according to the sequence which was chosen according to the defined sequence, and which used one and

was defined [from] among said 2nd information among said 2nd key It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. The decode approach characterized by decoding and obtaining said data using said 1st key which repeated said selection and said judgment until the 1st key judged to be a right thing was obtained, and was obtained as a right thing.

[Claim 14] The 2nd information which enciphered, respectively and was acquired from the record medium with two or more 2nd keys which were able to define beforehand the 1st information which was read at least, and which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging Or it was built in the driving gear of said record medium, while telling the 2nd unit through the CPU bus of a calculating machine from the 1st unit connected to the driving gear of said record medium, without minding the CPU bus of a calculating machine At least about said 2nd and 3rd information It tells insurance, without being acquired from the exterior. In said 2nd unit While decoding the 1st one enciphered key which was chosen [from] according to the sequence which was chosen according to the defined sequence, and which used one and was defined [from] among said 2nd information among said 2nd key It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right

thing. The decode approach characterized by decoding and obtaining said data using said 1st key which repeated said selection and said judgment until the 1st key judged to be a right thing was obtained, and was obtained as a right thing.

[Claim 15] The 1st information which enciphered the 3rd key with the 1st key and was acquired, and said 1st key are enciphered with two or more 2nd keys which were able to be defined beforehand, respectively. Read these information at least and it is read from the record medium which memorized the 4th information which enciphered the 2nd acquired information, the 3rd information used for a key judging, and data with said 3rd key, and was acquired at least. While decoding the 1st one enciphered key which was chosen [from] according to the sequence which was chosen according to the defined sequence, and which used one and was defined [from] among said 2nd information among said 2nd key It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. The decode approach characterized by repeating said selection and said judgment until the 1st key judged to be a right thing is obtained, being able to decode said 3rd key using said 1st key obtained as a right thing, and decoding and obtaining said data using said 3rd obtained key.

[Claim 16] The 2nd information which enciphered, respectively and was acquired from the record medium with two or more 2nd keys which were able to define

beforehand the 1st information which was read at least, and which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging Or it was built in the driving gear of said record medium, it is told to the driving gear of said record medium through the CPU bus of a calculating machine from the unit for a bus transfer connected without minding the CPU bus of a calculating machine. Are decryption unit equipment which decodes said data based on these information, and the CPU bus of said calculating machine is minded between said units for a bus transfer. The means for delivering said 2nd and 3rd information to insurance at least, without being acquired from the exterior, One is used. it chose according to the sequence defined [from] among said 2nd key memorized by a storage means to memorize at least one of said the 2nd key, and said storage means -- While decoding the 1st one enciphered key which was chosen [from] according to the defined sequence among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. The 1st decode means which repeats said selection and said judgment until the 1st key judged to be a right thing is obtained, Decryption unit equipment characterized by having the 2nd decode means which decodes and obtains said data using said 1st key obtained as a right thing by this 1st decode means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the manufacture approach of the encryption approach for preventing the copy from a record medium to the data by which digital recording was carried out, the decode approach, a record regenerative apparatus, decode equipment, decryption unit equipment, a record medium, and a record medium, and the management method of a key.

[0002]

[Description of the Prior Art] With the record medium of voice or an image, there are a compact disk and a laser disk as a medium which records the digitized information (for example, a document, voice, an image, a program, etc.) conventionally. Moreover, there are a floppy disk and a hard disk in the program of a computer etc., or the record medium of data. Moreover, in addition to these record media, DVD (digital video disc) which is a mass record medium is developed.

[0003] In the above various digital recording media, copying the recorded data to

other media, since the digital data (compression, coding, etc. be carried out and what can be decoded be included) as it is be recorded when recording can be copied having no loss of tone quality or image quality, and easily, it could make the duplicate in large quantities, and had problems, such as infringement of copyright.

[0004]

[Problem(s) to be Solved by the Invention] As mentioned above, when copying from a digital recording medium, it can copy there being no degradation of tone quality or image quality, and maintaining the tone quality and image quality of a master. For this reason, there were problems, like the illegal action which sells media, without paying the charge of writing becomes possible by the unjust copy called a pirate edition.

[0005] This invention was made in consideration of the above-mentioned situation, and aims at offering the manufacture approach of the encryption approach for preventing the unjust copy from a record medium by which digital recording was carried out, the decode approach, a record regenerative apparatus, decode equipment, decryption unit equipment, a record medium, and a record medium, and the management method of a key.

[0006]

[Means for Solving the Problem] The encryption approach concerning this

invention (claim 1) is characterized by enciphering data with the 1st key and enciphering, respectively with two or more 2nd keys which were able to define said 1st key beforehand.

[0007] The record medium concerning this invention (claim 2) is characterized by recording at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively.

[0008] The manufacture approach of the record medium concerning this invention (claim 3) is characterized by recording at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively in the same record medium.

[0009] The decode approach concerning this invention (claim 4) inputs at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively. Said 1st key can be decoded using at least one of said the 2nd key, and after judging by the predetermined approach that the 1st obtained key is a right thing, it is characterized by using this 1st key, and decoding and obtaining said data.

[0010] An input means by which the decode equipment concerning this invention

(claim 5) inputs at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively, Said 1st key is decoded and obtained based on the information inputted from said input means using at least one of said the 2nd key within a storage means to memorize at least one of said the 2nd key, and this storage means. After judging by the predetermined approach that the 1st obtained key is a right thing, it is characterized by having used this 1st key and having a decode means to decode and obtain said data.

[0011] A read-out means by which the record regenerative apparatus concerning this invention (claim 6) reads these information from the record medium which memorized at least the information which enciphered the information which enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively at least, Said 1st key is decoded and obtained based on the information read from said read-out means using at least one of said the 2nd key within a storage means to memorize at least one of said the 2nd key, and this storage means. After judging by the predetermined approach that the 1st obtained key is a right thing, it is characterized by having used this 1st key and having a decode means to decode and obtain said data.

[0012] The management method of the key concerning this invention (claim 7)

makes two or more 2nd keys beforehand set to the 1st manager keep it at least. It is characterized by making the 2nd manager manage at least the information which enciphered data with the 1st key, and the information which enciphered said 1st key with said two or more 2nd keys defined beforehand, respectively, and making the 3rd manager manage at least one of said the 2nd key.

[0013] According to this invention, only a just thing with at least one of two or more 2nd keys can obtain the plane data of the data which could obtain the 1st key, therefore were enciphered with the 1st key.

[0014] Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept.

[0015] The decode equipment concerning this invention (claim 8) The read-out means which reads these information from the record medium which memorized at least the 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging at least, One is used. it chose according to the sequence defined [from] among said 2nd key memorized by a storage means to memorize at least one of said the 2nd key, and said storage means -- While decoding the 1st one enciphered key which was chosen [from] according to the defined sequence among said 2nd

information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. It is characterized by having the 1st decode means which repeats said selection and said judgment, and the 2nd decode means which decodes and obtains said data using said 1st key obtained as a right thing by this 1st decode means until the 1st key judged to be a right thing is obtained.

[0016] This invention (claim 9) the 2nd information which enciphered, respectively and was acquired from the record medium with two or more 2nd keys which were able to define beforehand the 1st information which was read at least, and which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging It tells the 2nd unit through the CPU bus of a calculating machine from the 1st unit connected to the driving gear of said record medium, without minding the CPU bus of a calculating machine or it was built in the driving gear of said record medium. It is decode equipment which decodes said data at least in said 2nd unit. Said 1st unit While telling said 1st, 2nd, and 3rd information to said 2nd unit through the CPU bus of said calculating machine, at least about said 2nd and 3rd information It has a means for telling insurance, without being acquired from the exterior. Said 2nd unit While receiving said 1st, 2nd, and 3rd information from said 1st unit through the CPU bus of said calculating machine, at least about

said 2nd and 3rd information The means for receiving safely, without being acquired from the exterior, and a storage means to memorize at least one of said the 2nd key, While decoding the 1st one enciphered key which was chosen according to the sequence which was chosen according to the sequence defined [from] among said 2nd key memorized by said storage means, and which used one and was defined [from] among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. It is characterized by having the 1st decode means which repeats said selection and said judgment, and the 2nd decode means which decodes and obtains said data using said 1st key obtained as a right thing by this 1st decode means until the 1st key judged to be a right thing is obtained.

[0017] The decode equipment concerning this invention (claim 10) The 1st information which enciphered the 3rd key with the 1st key and was acquired, and said 1st key are enciphered with two or more 2nd keys which were able to be defined beforehand, respectively. The read-out means which reads these information from the record medium which memorized the 4th information which enciphered the 2nd acquired information, the 3rd information used for a key judging, and data with said 3rd key, and was acquired at least at least, One is used. it chose according to the sequence defined [from] among said 2nd key

memorized by a storage means to memorize at least one of said the 2nd key, and said storage means -- While decoding the 1st one enciphered key which was chosen [from] according to the defined sequence among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. The 1st decode means which repeats said selection and said judgment until the 1st key judged to be a right thing is obtained, It is characterized by having the 2nd decode means which decodes and obtains said 3rd key using said 1st key obtained as a right thing by this 1st decode means, and the 3rd decode means which decodes and obtains said data using said 3rd key obtained by this 2nd decode means.

[0018] This invention was read from the record medium at least. The 4th information which enciphered the 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered the 3rd key with the 1st key and was acquired, and said 1st key, the 3rd information used for a key judging, and data with said 3rd key, and was acquired It tells the 2nd unit through the CPU bus of a calculating machine from the 1st unit connected to the driving gear of said record medium, without minding the CPU bus of a calculating machine or it was built in the driving gear of said record medium. It is decode equipment which decodes said data at least in said 2nd unit. Said 1st

unit While telling said 1st, 2nd, 3rd, and 4th information to said 2nd unit through the CPU bus of said calculating machine, at least about said 2nd and 3rd information It has a means for telling insurance, without being acquired from the exterior. Said 2nd unit While receiving said 1st, 2nd, 3rd, and 4th information from said 1st unit through the CPU bus of said calculating machine, at least about said 2nd and 3rd information The means for receiving safely, without being acquired from the exterior, and a storage means to memorize at least one of said the 2nd key, While decoding the 1st one enciphered key which was chosen according to the sequence which was chosen according to the sequence defined [from] among said 2nd key memorized by said storage means, and which used one and was defined [from] among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. The 1st decode means which repeats said selection and said judgment until the 1st key judged to be a right thing is obtained, It is characterized by having the 2nd decode means which decodes and obtains said 3rd key using said 1st key obtained as a right thing by this 1st decode means, and the 3rd decode means which decodes and obtains said data using said 3rd key obtained by this 2nd decode means.

[0019] Said 3rd information is the information which enciphered said 1st key for said 1st key itself, and was acquired preferably. Said 1st decode means When

the key which decoded one of said 2nd information and was obtained using one of said the 2nd key memorized by said storage means, and the key which decoded said said 3rd information and was obtained using this key are in agreement, it judges with this key being the 1st key of the right.

[0020] Preferably, said data contain at least one of key information, a document, voice, an image, and programs.

[0021] The decode approach concerning this invention (claim 13) These information is read from the record medium which memorized at least the 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging at least. While decoding the 1st one enciphered key which was chosen [from] according to the sequence which was chosen according to the defined sequence, and which used one and was defined [from] among said 2nd information among said 2nd key It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. Said selection and said judgment are repeated until the 1st key judged to be a right thing is obtained, and it is characterized by decoding and obtaining said data using said 1st key obtained as a right thing.

[0022] The decode approach concerning this invention (claim 14) was read from the record medium at least. The 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging Or it was built in the driving gear of said record medium, while telling the 2nd unit through the CPU bus of a calculating machine from the 1st unit connected to the driving gear of said record medium, without minding the CPU bus of a calculating machine At least about said 2nd and 3rd information It tells insurance, without being acquired from the exterior. In said 2nd unit While decoding the 1st one enciphered key which was chosen [from] according to the sequence which was chosen according to the defined sequence, and which used one and was defined [from] among said 2nd information among said 2nd key It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. Said selection and said judgment are repeated until the 1st key judged to be a right thing is obtained, and it is characterized by decoding and obtaining said data using said 1st key obtained as a right thing.

[0023] The decode approach concerning this invention (claim 15) The 1st information which enciphered the 3rd key with the 1st key and was acquired, and

said 1st key are enciphered with two or more 2nd keys which were able to be defined beforehand, respectively. Read these information at least and it is read from the record medium which memorized the 4th information which enciphered the 2nd acquired information, the 3rd information used for a key judging, and data with said 3rd key, and was acquired at least. While decoding the 1st one enciphered key which was chosen [from] according to the sequence which was chosen according to the defined sequence, and which used one and was defined [from] among said 2nd information among said 2nd key It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. It is characterized by repeating said selection and said judgment until the 1st key judged to be a right thing is obtained, being able to decode said 3rd key using said 1st key obtained as a right thing, and decoding and obtaining said data using said 3rd obtained key.

[0024] The decode approach concerning this invention was read from the record medium at least. The 4th information which enciphered the 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered the 3rd key with the 1st key and was acquired, and said 1st key, the 3rd information used for a key judging, and data with said 3rd key, and was acquired Or it was built in the driving gear of said record medium, while telling the 2nd unit through

the CPU bus of a calculating machine from the 1st unit connected to the driving gear of said record medium, without minding the CPU bus of a calculating machine At least about said 2nd and 3rd information It tells insurance, without being acquired from the exterior. In said 2nd unit While decoding the 1st one enciphered key which was chosen [from] according to the sequence which was chosen according to the defined sequence, and which used one and was defined [from] among said 2nd information among said 2nd key It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. It is characterized by repeating said selection and said judgment until the 1st key judged to be a right thing is obtained, being able to decode said 3rd key using said 1st key obtained as a right thing, and decoding and obtaining said data using said 3rd obtained key.

[0025] The 2nd information which enciphered, respectively and was acquired from the record medium with two or more 2nd keys which were able to define beforehand the 1st information which was read at least, and which enciphered data with the 1st key and was acquired, and said 1st key, and the 3rd information used for a key judging this invention (claim 16) Or it was built in the driving gear of said record medium, it is told to the driving gear of said record medium through the CPU bus of a calculating machine from the unit for a bus transfer connected without minding the CPU bus of a calculating machine. Are

decryption unit equipment which decodes said data based on these information, and the CPU bus of said calculating machine is minded between said units for a bus transfer. The means for delivering said 2nd and 3rd information to insurance at least, without being acquired from the exterior, One is used. it chose according to the sequence defined [from] among said 2nd key memorized by a storage means to memorize at least one of said the 2nd key, and said storage means -- While decoding the 1st one enciphered key which was chosen [from] according to the defined sequence among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. It is characterized by having the 1st decode means which repeats said selection and said judgment, and the 2nd decode means which decodes and obtains said data using said 1st key obtained as a right thing by this 1st decode means until the 1st key judged to be a right thing is obtained.

[0026] This invention was read from the record medium at least. The 4th information enciphered and acquired with said 3rd key the 2nd information which enciphered, respectively and was acquired with two or more 2nd keys which were able to define beforehand the 1st information which enciphered the 3rd key with the 1st key and was acquired, and said 1st key, the 3rd information used for a key judging, and data Or it was built in the driving gear of said record medium,

it is told to the driving gear of said record medium through the CPU bus of a calculating machine from the unit for a bus transfer connected without minding the CPU bus of a calculating machine. Are decryption unit equipment which decodes said data based on these information, and the CPU bus of said calculating machine is minded between said units for a bus transfer. The means for delivering said 2nd and 3rd information to insurance at least, without being acquired from the exterior, One is used. it chose according to the sequence defined [from] among said 2nd key memorized by a storage means to memorize at least one of said the 2nd key, and said storage means -- While decoding the 1st one enciphered key which was chosen [from] according to the defined sequence among said 2nd information It judges whether this 1st key obtained by said decode based on this decode result and said 3rd information at least is a right thing. The 1st decode means which repeats said selection and said judgment until the 1st key judged to be a right thing is obtained, It is characterized by having the 2nd decode means which decodes and obtains said 3rd key using said 1st key obtained as a right thing by this 1st decode means, and the 3rd decode means which decodes and obtains said data using said 3rd key obtained by this 2nd decode means.

[0027] The record medium concerning this invention is characterized by recording at least the information which enciphered the information which

enciphered data with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively, and the information (for example, information which enciphered said 1st key for said 1st key itself) used for a key judging.

[0028] The record medium concerning this invention is characterized by recording at least the information which enciphered the information which enciphered the 3rd key with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively, and the information which enciphered data with said 3rd key.

[0029] The record medium concerning this invention is characterized by to record at least the information which enciphered the information which enciphered the 3rd key with the 1st key, and said 1st key with two or more 2nd keys which were able to be defined beforehand, respectively, the information (for example, the information which enciphered said 1st key for said 1st key itself) used for a key judging, and the information which enciphered data with said 3rd key.

[0030] According to this invention, only a just thing with at least one of two or more 2nd keys can obtain the plane data of the data which could obtain the 1st key, therefore were enciphered with the 1st key. Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be

kept.

[0031] Moreover, even if it saves the data which flow to the signal line which connects an encryption unit and a decryption unit according to this invention Information required in order to encipher these data and to encipher these data The saved data cannot be reproduced or used even if the 2nd key in a decode unit (master key) was torn, since it is not generated based on a random number and was not able to reappear behind. Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept. Moreover, according to this invention, an encryption unit and a decryption unit should just exchange an encryption unit and a decryption unit, even if a code is broken, since the part used as the core of the playback part of a digital recording playback device can design independently.

[0032] Moreover, the digital data with which this invention 1 was enciphered by the 1st predetermined session key, It is the decode approach for obtaining the plaintext of this digital data from the record medium which recorded the 1st session key enciphered with the master key defined beforehand. In a decryption unit, the 2nd session key is generated based on a predetermined random number. The 2nd generated session key is decoded with said master key. From a decryption unit to an encryption unit The 2nd session key decoded with said master key which transmitted the 2nd session key decoded with said master key,

and was transmitted in the encryption unit is enciphered with said master key. Said 2nd session key which took out said 2nd session key and was taken out in the encryption unit is used. The 1st session key enciphered with said master key read from said record medium is enciphered. To the decryption unit, were enciphered using the 2nd session key from the encryption unit. The 1st session key enciphered with said master key is transmitted. In a decryption unit The 1st session key which was enciphered using said 2nd transmitted session key and which was enciphered with said master key Decode using said 2nd session key and the 1st session key enciphered with said master key which took out the 1st session key enciphered with said master key, and was taken out further is decoded with said master key. It is characterized by decoding the digital data enciphered by said 1st session key which took out said 1st session key and was read from said record medium using said 1st taken-out session key, and obtaining the plaintext of said digital data.

[0033] The digital data with which this invention 2 was enciphered by the 1st predetermined session key, The 1st session key enciphered with the predetermined master key of two or more master keys defined beforehand, It is the decode approach for obtaining the plaintext of this digital data from the record medium which recorded the 1st session key enciphered for the 1st session key itself. In a decryption unit, the 2nd session key is generated based

on a predetermined random number. The 2nd generated session key is decoded with the master key which was able to be defined beforehand. The 2nd session key decoded with said master key defined beforehand is transmitted to an encryption unit from a decryption unit. The 2nd session key decoded with said master key which was transmitted in the encryption unit, and which was defined beforehand is enciphered with said master key defined beforehand. Said 2nd session key which took out said 2nd session key and was taken out in the encryption unit is used. While enciphering the 1st session key enciphered with said predetermined master key read from said record medium The 1st session key enciphered for said 1st session key itself which was read from said record medium is enciphered using said 2nd taken-out session key. While transmitting the 1st session key which was enciphered from the encryption unit to the decryption unit using the 2nd session key and which was enciphered with said predetermined master key The 1st session key which was enciphered using the 2nd session key and which was enciphered for said 1st session key itself is transmitted. In the decryption unit, were enciphered using said 2nd transmitted session key. While taking out the 1st session key which decoded the 1st session key enciphered with said predetermined master key using said 2nd session key, and was enciphered with said predetermined master key The 1st session key which was enciphered using said 2nd transmitted session key and which was

enciphered for said 1st session key itself Decode using said 2nd session key and the 1st session key enciphered for said 1st session key itself is taken out. With the 1st session candidate key which decoded the 1st session key enciphered with said predetermined master key taken out in the decryption unit in either of two or more master keys which were able to be defined beforehand The 1st session key enciphered for said 1st session key itself which was taken out The 1st session candidate key is used as said 1st predetermined session key. this -- the case where what was decoded by the 1st session candidate key is in agreement -- this -- It is characterized by decoding the digital data enciphered by said 1st session key read from said record medium using said 1st obtained session key, and obtaining the plaintext of said digital data.

[0034] The digital data with which this invention 3 was enciphered by the 1st predetermined session key, The 1st session key enciphered with two or more master keys defined beforehand, respectively, It is the decode approach for obtaining the plaintext of this digital data from the record medium which recorded the 1st session key enciphered for the 1st session key itself. In a decryption unit, the 2nd session key is generated based on a predetermined random number. The 2nd generated session key is decoded with the master key which was able to be defined beforehand. The 2nd session key decoded with the master key defined beforehand is transmitted to an encryption unit from a decryption unit.

The 2nd session key decoded with the master key which was transmitted in the encryption unit, and which was defined beforehand is enciphered with the master key which was able to be defined beforehand. While enciphering the 1st session key enciphered with said master key read from said record medium using said 2nd session key which took out said 2nd session key and was taken out in the encryption unit The 1st session key enciphered for said 1st session key itself which was read from said record medium is enciphered using said 2nd taken-out session key. While transmitting the 1st session key which was enciphered from the encryption unit to the decryption unit using the 2nd session key and which was enciphered with said master key The 1st session key which was enciphered using the 2nd session key and which was enciphered for said 1st session key itself is transmitted. In the decryption unit, were enciphered using said 2nd transmitted session key. While taking out the 1st session key which decoded the 1st session key enciphered with said master key using said 2nd session key, and was enciphered with said master key The 1st session key which was enciphered using said 2nd transmitted session key and which was enciphered for said 1st session key itself Decode using said 2nd session key and the 1st session key enciphered for said 1st session key itself is taken out. With the 1st session candidate key which decoded the 1st session key enciphered with said master key taken out in the decryption unit with the master

key which was able to be defined beforehand The 1st session key enciphered for said 1st session key itself which was taken out The 1st session candidate key is used as said 1st predetermined session key. this -- the case where what was decoded by the 1st session candidate key is in agreement -- this -- It is characterized by decoding the digital data enciphered by said 1st session key read from said record medium using said 1st obtained session key, and obtaining the plaintext of said digital data.

[0035] The digital data with which this invention 4 was enciphered by the 1st predetermined session key, The 1st session key enciphered with two or more master keys defined beforehand, respectively, It is the decode approach for obtaining the 1st session key used for decode of this digital data from the record medium which recorded the 1st session key enciphered for the 1st session key itself. Come out of and decode what the 1st session key enciphered with said master key was beforehand determined of said two or more master keys as, and the 1st session candidate key is generated. The 1st session key enciphered for said 1st session key itself is decoded using said 1st generated session candidate key. With said 1st session candidate key this -- when the 1st session key which was decoded using the 1st session candidate key and which was enciphered for said 1st session key itself is compared and it is in agreement by said comparison, it is characterized by determining said 1st session candidate

key as said 1st predetermined session key.

[0036] It is characterized by this invention 5 being the integrated circuit device in which said encryption unit and said decryption unit were formed independently in the above-mentioned invention 1 thru/or any one invention of 3, respectively.

[0037] Transmission to which this invention 6 is carried out between said encryption units and said decryption units in the above-mentioned invention 1 thru/or any one invention of 3 is CPU. It is characterized by being carried out using BUS.

[0038] This invention 7 is characterized by said predetermined random number being what changes whenever it reproduces said record medium at least in the above-mentioned invention 1 thru/or any one invention of 3.

[0039] This invention 8 is characterized by generating said predetermined random number based on the hour entry acquired to predetermined timing in the above-mentioned invention 1 thru/or any one invention of 3.

[0040] Predetermined timing is the timing by which the driving gear was equipped with said record medium, for example.

[0041] This invention 9 is characterized by said data being a thing containing at least one of key information, a document, voice, an image, and programs in the above-mentioned invention 1 thru/or any one invention of 4.

[0042] The digital data with which this invention 10 was enciphered by the 1st

predetermined session key, It is decode equipment for obtaining the plaintext of this digital data from the record medium which recorded the 1st session key enciphered with the master key defined beforehand. The 2nd session key generation means which generates the 2nd session key which is prepared in a decryption unit and is different according to predetermined conditions, Said 2nd generated session key is decoded with said master key within said decryption unit. The means which takes out said 2nd session key by transmitting this data into an encryption unit and enciphering with said master key within said encryption unit, A means to encipher said 1st session key enciphered with said master key read from said record medium using the 2nd session key taken out by this means, and to transmit to said decryption unit, A means to use and decode said master key further and to obtain said 1st session key after decoding the 1st [which was transmitted into the decryption unit by this means] enciphered session key using the 2nd session key generated within said decryption unit, It is characterized by having decoded the digital data enciphered by said 1st session key read from said record medium using said 1st session key obtained by this means, and having a means to obtain the plaintext of said digital data.

[0043] This invention 11 is characterized by generating the 2nd different session key according to a hour entry, whenever said 2nd session key generation means

performs decode actuation of said record medium in the above-mentioned invention 10.

[0044] The record medium concerning this invention 12 is characterized by recording the 1st session key enciphered, respectively with two or more master keys beforehand determined as the digital data enciphered by the 1st predetermined session key, and the 1st session key enciphered for the 1st session key itself.

[0045] A record medium is applicable to various things, such as DVD, CD-ROM, a floppy disk, and a hard disk.

[0046] In addition, each invention concerning equipment [more than] is materialized also as invention concerning an approach, or invention concerning a storage, respectively, and each invention concerning the above approach is materialized also as invention concerning equipment, or invention concerning a storage, respectively.

[0047] Even if it saves the data which flow to the signal line which connects an encryption unit and a decryption unit according to this invention Information required in order to encipher these data and to encipher these data The saved data cannot be reproduced or used even if the master key in a decode unit was torn, since it is not generated based on a random number and was not able to reappear behind.

[0048] Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept.

[0049] Moreover, according to this invention, an encryption unit and a decryption unit should just exchange an encryption unit and a decryption unit, even if a code is broken, since the part used as the core of the playback part of a digital recording playback device can design independently.

[0050] Moreover, the digital data which was enciphered by the record medium by the 1st predetermined session key according to this invention, By recording the 1st session key enciphered with the predetermined master key of two or more master keys defined beforehand, and the 1st session key enciphered for the 1st session key itself Even if said predetermined master keys are any of two or more master keys, the 1st session key can be taken out by the decryption unit with two or more master keys, and data can be decoded by this 1st session key.

[0051] Moreover, the digital data which was enciphered by the record medium by the 1st predetermined session key according to this invention, By recording the 1st session key enciphered with two or more master keys defined beforehand, respectively, and the 1st session key enciphered for the 1st session key itself The 1st session key can be taken out by the decryption unit with at least at least one either of said two or more master keys, and data can be decoded by this 1st session key.

[0052]

[Embodiment of the Invention] Hereafter, the gestalt of implementation of invention is explained, referring to a drawing.

[0053] It is EK about the actuation which enciphers a certain data a with this operation gestalt using Key K. It is DK about the actuation which expresses it as (a) and decrypts a certain data a using Key K. It is expressed as (a). By using this expression, the actuation which enciphers and decodes a certain data a using Key K is expressed in DK (EK (a)), for example.

[0054] Moreover, with this operation gestalt, it may return to the data of even if it enciphers the data which decrypted a certain data first and were decrypted after that. This is based on a decryption of data having an operation equivalent to encryption on the property of a code. That is, the data decrypted first are obtained by enciphering the data decrypted when the key used for the decryption had to be found and the key was found, in order to return the decrypted data. This actuation sets a cryptographic key to x, and data are expressed with y, then Ex =(Dx (y)) y.

[0055] This operation gestalt explains the image data compressed and enciphered according to the data compression specification of MPEG 2 recorded on DVD taking the case of the system read, decoded, decoded and reproduced.

[0056] (1st operation gestalt) The 1st operation gestalt is explained hereafter.

[0057] Drawing 1 is the block diagram showing the structure of a system concerning the 1st operation gestalt of this invention. Moreover, an example of actuation of this operation gestalt is shown in the flow chart of drawing 2 .

[0058] The system concerning this operation gestalt is the so-called CPU of CPU (not shown) used for the playback which it had in computers, such as a personal computer. The data (ESK mentioned later (Data)) which are connected to BUS and enciphered are CPU. It has the configuration which flows a BUS top. In addition, drawing 1 shows only the part about CPU used for playback.

[0059] The system applied to this operation gestalt as shown in drawing 1 is [the DVD driving gear (not shown) which reads data from DVD101, and] CPU to this DVD driving gear. Or it connected without minding BUS, it has the encryption unit 107 and the decryption unit 114 which were built in the DVD driving gear.

[0060] The encryption unit 107 and the decryption unit 114 are CPU. It connects with BUS110. The output of the data from the decryption unit 114 is CPU. It is carried out through I/O Ports other than BUS etc. That is, at this operation gestalt, I/O of data is CPU. Although carried out without minding BUS, in the data transfer between the encryption unit 107 and the decryption unit 114, it is CPU. BUS is used.

[0061] The encryption unit 107 is equipped with the recovery / error correction circuit 117, the recovery / error correction circuit 118, and the encryption circuit

104. Although two encryption circuits 104 are shown in the encryption unit 107 in drawing 1 , it shall be one encryption circuit in fact. The encryption unit 107 shall be formed as one independent IC chip. In addition, in the encryption unit 107, it does not have a recovery / error correction circuit 117, and the recovery / error correction circuit 118, but sides (inside of a DVD driving gear), such as a unit of the preceding paragraph, may be equipped with it.

[0062] On the other hand, the decryption unit 114 is equipped with the decryption circuit 112 and the session key generation circuit 111 which generates 2nd session key SK '. Moreover, with this operation gestalt, it shall have the conversion circuit 116 which changes into an analog the decoder circuit 115 and the decoded image data of MPEG from digital one in the decryption unit 114. Although four decryption circuits 112 are shown in the decryption unit 114 in drawing 1 , it shall be one decryption circuit in fact. The decryption unit 114 shall be formed as one independent IC chip.

[0063] Moreover, the master key mentioned later is registered into the encryption unit 107 and the decryption unit 114 (made). The master key shall be recorded on the field to which the interior of a chip was kept secret so that a user could not take out intentionally in the chip of an encryption unit, and each chip of a decryption unit so that a user cannot acquire from the exterior.

[0064] In addition, the control section which is not illustrated shall manage the

whole control. A control section is realizable by performing a program by CPU of the computer concerned. As an example of control by this control section, they are the directions about read-out of the data from DVD, assignment of the data transmission point, the directions about the data output from the decryption unit 114, etc. Moreover, the trigger of starting of this control section can consider the case where it is carried out by the user through a user interface, the case where it is applied from the process in a certain application program, etc.

[0065] SK and the 2nd session key are expressed with SK', and this operation gestalt expresses [the 1st session key] MK and image data (namely, data of the enciphered bundle ball) for a master key by Data. Each of these is plaintexts.

[0066] The inside of drawing 1 and 102 are the 1st session key SK. Master key MK EMK (SK) used, enciphered and generated 103 is the 1st session key SK about image data Data. ESK (Data) used, enciphered and generated 105 is a master key MK. 106 2nd session key SK ' 108 DMK (SK ') which decoded 2nd session key SK ' using the master key MK 109 is a master key MK. About ESK' (EMK (SK)) which enciphered the 1st session key EMK (SK) used and enciphered using 2nd session key SK ', 113 is the 1st session key SK. It expresses, respectively.

[0067] As shown in drawing 3 , it is the 1st session key SK on DVD101. Master key MK EMK (SK) enciphered [was used and] and generated is the 1st session

key SK about image data Data to the key record section (lead-in groove area) of a most-inner-circumference part. ESK (Data) enciphered [was used and] and generated shall be recorded on the data storage area (data area).

[0068] Hereafter, actuation of this operation gestalt is explained, referring to the flow chart of drawing 2 .

[0069] Master key MK currently recorded on DVD101 by the DVD driving gear which is not illustrated at step S1 The 1st session key EMK (SK) used and enciphered is read, and it incorporates in the code unit 107. The error correction in a recovery and data is performed by a recovery / error correction circuit 117 in that case.

[0070] On the other hand, in the decryption unit 114, 2nd session key SK ' is generated in the session key generation circuit 111 at step S2 by considering the hour entry from a random number (not shown), for example, a clock, as an input. And in the decryption circuit 112, 2nd generated session key SK ' is decoded using a master key MK, DMK (SK ') is generated, and it is CPU. It sends to the encryption unit 107 through BUS110.

[0071] The timing by which the signal which shows that the DVD driving gear was equipped with DVD101, for example as timing (for example, timing which inputs a hour entry) which generates the above-mentioned random number was asserted can be used.

[0072] Or the session key generation circuit 111 may consist of random number generators for for example, key length. In addition, when the random number by which all bits may be set to 0 or 1 generates a key, it is necessary to carry out check processing etc. so that no bits may be set to 0 or 1.

[0073] At step S3, it sets in the encryption circuit 104 in the code unit 107, and is CPU. In DMK (SK ') received through BUS110, it is MK about a master key. It uses and enciphers. That is, 2nd session key SK ' generated in the session key generation circuit 111 in the decryption unit 114 can be obtained by EMK(DMK (SK ')) =SK '.

[0074] Here, 2nd session key SK ' generated in the session key generation circuit 111 is CPU. It is made not to understand even if stolen on BUS110.

[0075] Next, the 1st [which was recorded on DVD101 in the code unit 107 by step S4 using 2nd session key SK ' obtained as mentioned above] enciphered session key EMK (SK) is enciphered, ESK' (EMK (SK)) is generated, and it is CPU about this. It sends to the decryption unit 114 through BUS110.

[0076] Next, in the decryption unit 114, it sets in the decryption circuit 112 at step S5, and is CPU. ESK' (EMK (SK)) received through BUS110 is decoded using 2nd session key SK ', and it is DSK' =(ESK') (EMK (SK)) EMK (SK).

******.

[0077] Furthermore, it is a master key MK about EMK (SK) obtained in the

decryption circuit 112. It uses and decodes and is DMK(EMK (SK)) =SK. It becomes and is the 1st session key SK. It can obtain.

[0078] It is the 1st session key SK as mentioned above. 1st session key SK currently recorded on DVD101 by the DVD driving gear which is not illustrated at step S6 after obtaining The image data ESK (Data) used and enciphered is read, and it incorporates in the code unit 107. The error correction in a recovery and data is performed by a recovery / error correction circuit 118 in that case. And it is CPU about ESK (Data). It sends to the encryption unit 107 through BUS110.

[0079] Next, in the decryption unit 114, it sets in the decryption circuit 112 at step S7, and is CPU. About ESK (Data) received through BUS110, it is the 1st session key SK. It uses and decodes, and it can be set to DSK(ESK (Data)) =Data, the enciphered image data can be decoded, and Data of a plaintext can be obtained.

[0080] And above-mentioned step S6 and above-mentioned step S7 are repeatedly performed until processing of the data (namely, ESK (Data)) which should be decoded, for example is completed or the termination of processing is required.

[0081] Image data Data obtained as mentioned above is decoded in the MPEG decoder circuit 115, when compressed according to the data compression specification of MPEG 2, and it is sent to image equipments, such as television

which is not illustrated after being changed into an analog signal by the D/A conversion circuit 116, and is reproduced.

[0082] In addition, the above-mentioned step S1 and steps S2 and S3 may perform whichever first.

[0083] Moreover, about activation of step S6 and step S7, ESK (Data) of a predetermined number is read at the approach of performing serially in the unit of one ESK (Data), or step S6, it once stores in a buffer etc., and the approach of decoding ESK (Data) in a buffer at step S7 next or the method of performing step S6 and step S7 in pipeline processing can be considered.

[0084] Moreover, in case image data ESK (Data) is passed to the MPEG decoder circuit 115 from the decryption circuit 112, you may pass in the unit of one Data and may pass in the unit of Data of a predetermined number.

[0085] When reproducing the medium which enciphered and recorded the digitized data as mentioned above according to this operation gestalt, (when decoding the enciphered data) CPU of a calculating machine The data decoded by BUS do not flow and it is CPU. 2nd session key SK ' used for encryption of the 1st session key required for decode of the enciphered data which flow to BUS For example, since it is generated based on the information which changes at every data playback like a hour entry, it is CPU like drawing 4 . It cannot be reproduced or used even if it saves the data which flow BUS110 from a signal

line 210 at the digital storage 211.

[0086] Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept.

[0087] Moreover, with this operation gestalt, the circuit used for encryption and a decryption should just exchange the decryption unit 114 (or the encryption unit 107 and the decryption unit 114), even if a code is broken, since the part used as the core of the playback part of digital recording playback devices, such as DVD, can design independently so that drawing 1 may show.

[0088] In addition, with this operation gestalt, although the code unit 107 shall have one encryption circuit, it may prepare two encryption circuits. Moreover, although the decryption unit 114 shall have one decryption circuit, it may be prepared as 2, 3, or four decryption circuits. It is desirable to make independent the encryption circuit and decryption circuit which correspond in these cases, or to share them by the set.

[0089] Moreover, when making independent a corresponding encryption circuit and a corresponding decryption circuit by the set, in the corresponding encryption circuit and corresponding decryption circuit which were made independent, a different cipher system from other encryption circuits and a decryption circuit may be adopted.

[0090] (2nd operation gestalt) Next, the 2nd operation gestalt is explained.

[0091] With this operation gestalt, for example, two or more master keys defined beforehand are prepared, and when assigning one or more master keys of them for every predetermined units, such as a manufacturer (or work / selling firm of DVD) of a decryption unit, a suitable example is explained.

[0092] Drawing 5 is the block diagram showing the structure of a system concerning the 2nd operation gestalt of this invention. Moreover, an example of actuation of this operation gestalt is shown in the flow chart of drawing 7 and drawing 8 .

[0093] The system concerning this operation gestalt is the so-called CPU of CPU (not shown) used for the playback which it had in computers, such as a personal computer. The data (ESK (Data)) which are connected to BUS and enciphered are CPU. It has the configuration which flows a BUS top. In addition, drawing 5 shows only the part about CPU used for playback.

[0094] The system applied to this operation gestalt as shown in drawing 5 is [the DVD driving gear (not shown) which data read from DVD101, and] CPU to this DVD driving gear. Or it connected without minding BUS, it has the encryption unit 107 and decryption unit 114a which were built in the DVD driving gear.

[0095] The encryption unit 107 and decryption unit 114a are CPU. It connects with BUS110. The output of the data from decryption unit 114a is CPU. It is carried out through I/O Ports other than BUS etc. That is, at this operation gestalt,

I/O of data is CPU. Although carried out without minding BUS, in the data transfer between the encryption unit 107 and decryption unit 114a, it is CPU. BUS is used.

[0096] The encryption unit 107 is equipped with the recovery / error correction circuit 117, the recovery / error correction circuit 118, and the encryption circuit 104. Although two encryption circuits 104 are shown in the encryption unit 107 in drawing 1 , it shall be one encryption circuit in fact. The encryption unit 107 shall be formed as one independent IC chip. In addition, in the encryption unit 107, it does not have a recovery / error correction circuit 117, and the recovery / error correction circuit 118, but sides (inside of a DVD driving gear), such as a unit of the preceding paragraph, may be equipped with it.

[0097] On the other hand, decryption unit 114a is equipped with the decryption circuit 112, the session key generation circuit 111 which generates 2nd session key SK ', and the key judging circuit 120.

[0098] Here, the example of 1 configuration of the key judging circuit 120 is shown in drawing 6 . This key judging circuit 120 is equipped with the decryption circuit 112, the comparator circuit 121, and the gate circuit 122. Moreover, with this operation gestalt, it shall have the conversion circuit 116 which changes into an analog the decoder circuit 115 and the decoded image data of MPEG from digital one in decryption unit 114a.

[0099] Although five decryption circuits 112 are shown in all in decryption unit 114a in drawing 5 and drawing 6 including two decryption circuits 112 in the key judging circuit 120, it shall be one decryption circuit in fact.

[0100] Decryption unit 114a shall be formed as one independent IC chip.

[0101] Moreover, the master key mentioned later is registered into the encryption unit 107 and decryption unit 114a (made). The master key shall be recorded on the field to which the interior of a chip was kept secret so that a user could not take out intentionally in the chip of an encryption unit, and each chip of a decryption unit so that a user cannot acquire from the exterior.

[0102] In addition, the control section which is not illustrated shall manage the whole control. A control section is realizable by performing a program by CPU of the computer concerned. As an example of control by this control section, they are the directions about read-out of the data from DVD, assignment of the data transmission point, the directions about the data output from decryption unit 114a, etc. Moreover, the trigger of starting of this control section can consider the case where it is carried out by the user through a user interface, the case where it is applied from the process in a certain application program, etc.

[0103] SK' and the t-th thing of the master keys whose n kinds exist are expressed with Mkt (it is t=1-n here), and this operation gestalt expresses [the 1st session key] image data (however, data of the enciphered bundle ball) for

SK and the 2nd session key by Data. Each of these is plaintexts.

[0104] The inside of drawing 1 and 102-1 are the 1st session key SK. EMKi (SK) enciphered and generated using the master key Mki 102-2 is the 1st session key SK. 1st session key SK ESk (SK) which enciphered in person and was generated 103 is the 1st session key SK about image data Data. ESK (Data) used, enciphered and generated In 105, 106 a master key Mkj 2nd session key SK ' 108 DMkj (SK ') which decoded 2nd session key SK ' using the master key Mkj 109-1 ESK' (EMKi (SK)) which enciphered the 1st session key EMKi (SK) enciphered using the master key Mki using 2nd session key SK' 109-2 is the 1st session key SK. About ESK' (ESk (SK)) which enciphered the 1st session key ESk (SK) enciphered in person using 2nd session key SK ', 113 is the 1st session key SK. It expresses, respectively.

[0105] 1st session key SK recorded on DVD101 here About a setup of the number of classes of EMKi (SK) enciphered and generated using the master key Mki, and the number of classes of a master key Mkj which it has in decryption unit 114a, as shown below, some approaches can be considered.

[0106] (Approach 1) One master key EMKi (SK) which makes i either1-n is recorded on DVD101, and it has n master keys Mkj corresponding to all of j= 1 - n in decryption unit 114a.

[0107] (Approach 2) n master keys EMKi corresponding to all of i= 1 - n (SK) are

recorded on DVD101, and it has one master key Mkj which makes j either1-n in decryption unit 114a.

[0108] (Approach 3) It is what extended the above-mentioned (approach 2), and n master keys EMKi corresponding to all of i= 1 - n (SK) are recorded on DVD101, and it has m master keys Mkj which make j the thing of m (2<m<n) class beforehand chosen from that of1-the n in decryption unit 114a.

[0109] in addition -- as a concrete numerical example -- n= 100, n= 400, etc. -- it is -- m= -- although it is 2, 3, 4, 10, etc., it is not limited to these.

[0110] (Approach 4) In the example which made DVD and the decryption unit reverse in the above-mentioned (approach 3), m master keys EMKi (SK) which make i the thing of m (2<m<n) class beforehand chosen from that of1-the n are recorded on DVD101, and it has n master keys Mkj corresponding to all of j= 1 - n in decryption unit 114a.

[0111] (Approach 5) n master keys EMKi corresponding to all of i= 1 - n (SK) are recorded on DVD101, and it has n master keys Mkj corresponding to all of j= 1 - n in decryption unit 114a.

[0112] In addition, in an approach 3 - an approach 5, the procedure for decode becomes the same.

[0113] As shown in drawing 3 , it is the 1st session key SK on DVD101. One piece (in the case of the above-mentioned (approach 1)) or EMKi [two or more

(in the case of above-mentioned - (approach 2) (approach 5))] (SK) enciphered and generated using the master key Mki To the key record section (lead-in groove area) of a most-inner-circumference part, it is the 1st session key SK about image data Data. ESK (Data) enciphered [was used and] and generated shall be recorded on the data storage area (data area).

[0114] Moreover, n pieces (in the case of the above-mentioned (approach 1), (an approach 4), and (an approach 5)), one piece (in the case of the above-mentioned (approach 2)), or m master keys (in the case of the above-mentioned (approach 3)) Mkj shall be registered into the decryption unit 114.

[0115] In addition, one master key defined beforehand shall be registered into the encryption unit 107.

[0116] Below, sequential explanation is given about the above-mentioned (approach 1), (an approach 2), and (an approach 3 - an approach 5).

[0117] First, actuation of this operation gestalt is explained, referring to the flow chart of drawing 7 and drawing 8 about the case of the above-mentioned (approach 1).

[0118] 1st session key SK currently recorded on DVD101 by the DVD driving gear which is not illustrated at step S11 The 1st session key ESk (SK) enciphered in person is read, and it incorporates in the code unit 107. The error

correction in a recovery and data is performed by a recovery / error correction circuit 117 in that case.

[0119] Moreover, at step S12, the 1st session key EMki (any one of i(SK) = 1 - the n; here, i is strange) which is recorded on DVD101 by the DVD driving gear which is not illustrated and which was enciphered using the master key Mki is read, and it incorporates in the code unit 107. The error correction in a recovery and data is performed by a recovery / error correction circuit 117 in that case.

[0120] On the other hand, at decryption unit 114a, 2nd session key SK ' is generated in the session key generation circuit 111 at step S13 by considering the hour entry from a random number (not shown), for example, a clock, as an input. And in the decryption circuit 112, 2nd generated session key SK ' is decoded using a master key Mkj (what j was beforehand determined as among1-n here), DMkj (SK ') is generated, and it is CPU. It sends to the encryption unit 107 through BUS110.

[0121] The timing by which the signal which shows that the DVD driving gear was equipped with DVD101, for example as timing (for example, timing which inputs a hour entry) which generates the above-mentioned random number was asserted can be used.

[0122] Or the session key generation circuit 111 may consist of random number generators for for example, key length. In addition, when the random number by

which all bits may be set to 0 or 1 generates a key, it is necessary to carry out check processing etc. so that no bits may be set to 0 or 1.

[0123] At step S14, it sets in the encryption circuit 104 in the code unit 107, and is CPU. A master key is enciphered for DMkj (SK ') received through BUS110 using a master key Mkj (what j was beforehand determined as among1-n here). That is, 2nd session key SK ' generated in the session key generation circuit 111 in decryption unit 114a can be obtained by EMkj =(DMkj) (SK ') SK '.

[0124] Here, 2nd session key SK ' generated in the session key generation circuit 111 is CPU. It is made not to understand even if stolen on BUS110.

[0125] Next, the 1st [which was recorded on DVD101 in the code unit 107 by step S15 using 2nd session key SK ' obtained as mentioned above] enciphered session key ESk (SK) is enciphered, ESK' (ESk (SK)) is generated, and it is CPU about this. It sends to decryption unit 114a through BUS110.

[0126] The 1st [which similarly was recorded on DVD101 in the code unit 107 by step S16 using 2nd session key SK ' obtained as mentioned above] enciphered session key EMki (SK) is enciphered, ESK' (EMki (SK)) is generated, and it is CPU about this. It sends to decryption unit 114a through BUS110.

[0127] Next, in decryption unit 114a, it sets in the decryption circuit 112 at step S17, and is CPU. ESK' (ESk (SK)) received through BUS110 is decoded using 2nd session key SK ', and it is DSK' =(ESK') (ESk (SK)) ESk (SK).

******.

[0128] Similarly, in decryption unit 114a, it sets in the decryption circuit 112 at step S18, and is CPU. ESK' (EMki (SK)) received through BUS110 is decoded using 2nd session key SK ', and it is DSK' =(ESK') (EMki) (SK) EMki (SK).

******.

[0129] The master key Mki used here when generating EMki (SK) uses the key judging circuit 120, as step S19 is shown below, since it is strange, and it is the 1st session key SK. It asks.

[0130] First, the principle of key judging processing is explained.

[0131] First, if EMki (SK) is decoded with all the master keys Mkj (j=1-n), respectively, it is Skij =DMkj (j(EMki) (SK) =1-n).

**********. here -- either of the Skij(s) (j=1-n) -- 1st session key SK it is .

[0132] next, any of Skij (j=1-n) generated using above ESk (SK) -- 1st session key SK it is -- or is investigated.

[0133] Then, when ESk (SK) is decoded by the candidate Skij of all the 1st session key (j=1-n), respectively, it is Sk"(i, j) =DSkij (ESk (SK)).

**********.

[0134] In i=j when the same master key Mkj as the master key Mki used here when generating EMki (SK) is used within a decryption unit, it is Sk"(i, j) =Skij =SK. It becomes.

[0135] therefore, every -- Skij (j=1-n) -- Sk -- " (i, j) -- investigating whether =Skij (j=1-n) is materialized -- Sk -- " (i, j) -- Skij which satisfies =Skij (j=1-n) 1st session key SK ****** -- it can obtain. In addition, this Skij The thing corresponding to j to give is the master key used this time.

[0136] It is as follows when this actuation is expressed in C using the notation of C.

for(i=1; i<n+1;i++){ DS1[i]=DMK[i](EMki(Sk)); DS2[i]=DSK[i](ESk(Sk)); if(DS1[i]==DS2[i]) { SK1=DS2[i]; break; } else EXIT_MISMATCH; }

In addition, the 2nd line of the above-mentioned procedure decodes EMki (SK) using Mki, and shows actuation of substituting this for DS1 [i].

[0137] The 3rd line of the above-mentioned procedure decodes ESk (SK) using Ski, and shows actuation of substituting this for DS2 [i].

[0138] The 4th line of the above-mentioned procedure shows actuation of DS1 [i] and DS2 [i] being in agreement, or judging how.

[0139] The 9th line of the above-mentioned procedure shows actuation in case DS1 [i] and DS2 [i] are inequalities.

[0140] Now, EMki (SK) is first decoded with a master key Mkj as j= 1, for example by the decryption circuit 112 in the key judging circuit 120 of drawing 6 , and it is Skij =DMkj (EMki (SK)).

******.

[0141] Next, it is Skij about ESk (SK) by the decryption circuit 112. It decodes and is Sk"=DSkij (ESk (SK)).

******.

[0142] next, the comparator circuit 121 -- above-mentioned Sk" and =Skij Skij or (drawing 6 (a)) Sk" (drawing 6 (b)) which compared, and controlled and held the gate circuit 122 when in agreement -- 1st session key SK ****** -- it outputs.

[0143] It is the 1st session key SK about the same actuation, making the above-mentioned j increase by every [1], when not in agreement. It repeats until it is obtained.

[0144] It is the 1st session key SK as mentioned above. 1st session key SK currently recorded on DVD101 by the DVD driving gear which is not illustrated at step S20 after obtaining The image data ESK (Data) used and enciphered is read, and it incorporates in the code unit 107. The error correction in a recovery and data is performed by a recovery / error correction circuit 118 in that case. And it is CPU about ESK (Data). It sends to the encryption unit 107 through BUS110.

[0145] Next, in decryption unit 114a, it sets in the decryption circuit 112 at step S21, and is CPU. About ESK (Data) received through BUS110, it is the 1st session key SK. It uses and decodes, and it can be set to DSK(ESK (Data)) =Data, the enciphered image data can be decoded, and Data of a plaintext can

be obtained.

[0146] And above-mentioned step S20 and above-mentioned step S21 are repeatedly performed until the data (namely, ESK (Data)) which should be decoded, for example are completed or the termination of processing is required.

[0147] Image data Data obtained as mentioned above is decoded in the MPEG decoder circuit 115, when compressed according to the data compression specification of MPEG 2, and it is sent to image equipments, such as television which is not illustrated after being changed into an analog signal by the D/A conversion circuit 116, and is reproduced.

[0148] In addition, the above-mentioned step S11, step S12, and steps S13 and S14 may perform any first.

[0149] Moreover, the above-mentioned step S15 and step S17, and steps S16 and S18 may perform any first.

[0150] Moreover, about activation of step S20 and step S21, ESK (Data) of a predetermined number is read at the approach of performing serially in the unit of one ESK (Data), or step S20, it once stores in a buffer etc., and the approach of decoding ESK (Data) in a buffer at step S21 next or the method of performing step S20 and step S21 in pipeline processing can be considered.

[0151] Moreover, in case image data ESK (Data) is passed to the MPEG decoder circuit 115 from the decryption circuit 112, you may pass in the unit of

one Data and may pass in the unit of Data of a predetermined number.

[0152] According to this operation gestalt as mentioned above, it is CPU like the 1st operation gestalt. It cannot be reproduced or used even if it saves the data which flow BUS.

[0153] Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept.

[0154] Moreover, the information which shows directly the master key used for enciphering the 1st session key recorded on the record medium according to this operation gestalt becomes it is unnecessary and possible [using it suitably within limits beforehand defined on the occasion of record to DVD etc., choosing a master key]. Or there is an advantage of being able to assign an usable master key for every predetermined units, such as work / selling firm of DVD.

[0155] Of course, the circuit used for encryption and a decryption also with this operation gestalt should just exchange decryption unit 114a (or the encryption unit 107 and decryption unit 114a), even if a code is broken, since the part used as the core of the playback part of digital recording playback devices, such as DVD, can design independently.

[0156] In addition, with this operation gestalt, although the encryption unit 107 shall have one encryption circuit, it may prepare two encryption circuits. Moreover, although decryption unit 114a shall have one decryption circuit, 2, 3, 4,

or five decryption circuits may be prepared. It is desirable to make independent the encryption circuit which corresponds in these cases, and a decryption circuit by the set.

[0157] Moreover, when making independent a corresponding encryption circuit and a corresponding decryption circuit by the set, in the corresponding encryption circuit and corresponding decryption circuit which were made independent, a different cipher system from other encryption circuits and a decryption circuit may be adopted.

[0158] Next, n EMKi(s) (SK) corresponding to [like] all of i= 1 - n in DVD101 mentioned above (approach 2) are recorded, and actuation of this operation gestalt is explained, referring to the flow chart of drawing 7 and drawing 8 about the case where it has one Mkj which makes j either1-n in decryption unit 114a.

[0159] 1st session key SK currently recorded on DVD101 by the DVD driving gear which is not illustrated at step S11 The 1st session key ESk (SK) enciphered in person is read, and it incorporates in the code unit 107. The error correction in a recovery and data is performed by a recovery / error correction circuit 117 in that case.

[0160] Moreover, at step S12, the 1st n session key EMki (i(SK) =1-n) which is recorded on DVD101 by the DVD driving gear which is not illustrated and which was enciphered using the master key Mki is read, and it incorporates in the code

unit 107. The error correction in a recovery and data is performed by a recovery / error correction circuit 117 in that case.

[0161] On the other hand, at decryption unit 114a, 2nd session key SK ' is generated in the session key generation circuit 111 at step S13 by considering the hour entry from a random number (not shown), for example, a clock, as an input. And in the decryption circuit 112, 2nd generated session key SK ' is decoded using a master key Mkj (what j was beforehand determined as among1-n here), DMkj (SK ') is generated, and it is CPU. It sends to the encryption unit 107 through BUS110.

[0162] The timing by which the signal which shows that the DVD driving gear was equipped with DVD101, for example as timing (for example, timing which inputs a hour entry) which generates the above-mentioned random number was asserted can be used.

[0163] At step S14, it sets in the encryption circuit 104 in the code unit 107, and is CPU. A master key is enciphered for DMkj (SK ') received through BUS110 using a master key Mkj (what j was beforehand determined as among1-n here). That is, 2nd session key SK ' generated in the session key generation circuit 111 in decryption unit 114a can be obtained by EMkj =(DMkj) (SK ') SK '.

[0164] Here, 2nd session key SK ' generated in the session key generation circuit 111 is CPU. It is made not to understand even if stolen on BUS110.

[0165] Next, the 1st [which was recorded on DVD101 in the code unit 107 by step S15 using 2nd session key SK ' obtained as mentioned above] enciphered session key ESk (SK) is enciphered, ESK' (ESk (SK)) is generated, and it is CPU about this. It sends to decryption unit 114a through BUS110.

[0166] The 1st n enciphered session key EMki (SK) which similarly was recorded on DVD101 in the code unit 107 by step S16 using 2nd session key SK ' obtained as mentioned above is enciphered, respectively, ESK' (EMki (SK)) is generated, and it is CPU about this. It sends to decryption unit 114a through BUS110.

[0167] Next, in decryption unit 114a, it sets in the decryption circuit 112 at step S17, and is CPU. ESK' (ESk (SK)) received through BUS110 is decoded using 2nd session key SK ', and it is DSK' =(ESK') (ESk (SK)) ESk (SK).

******.

[0168] Similarly, in decryption unit 114a, it sets in the decryption circuit 112 at step S18, and is CPU. n ESK(s)' (EMki (SK)) received through BUS110 is decoded using 2nd session key SK ', respectively, and it is DSK' =(ESK') (EMki) (SK) EMki (SK).

******.

[0169] Here, the master key Mki used about each of n EMki(s) (i(SK) =1-n) currently recorded on DVD101 when generating it is strange, and it is turned out

which is the thing corresponding to the master key Mkj which it had in decryption unit 114a. Then, in step S19, as shown below, the key judging circuit 120 is used, and it is the 1st session key SK. It asks.

[0170] First, the principle of key judging processing is explained.

[0171] First, when all EMki(s) (i(SK) =1-n) are decoded with a master key Mkj, respectively, it is Skij=DMkj (i(EMki) (SK) =1-n).

**********. here -- either of the Skij(s) (i=1-n) -- 1st session key SK it is .

[0172] next, any of Skij (i=1-n) generated using above ESk (SK) -- 1st session key SK it is -- or is investigated.

[0173] Then, when ESk (SK) is decoded by the candidate Skij of all the 1st session key (i=1-n), respectively, it is Sk"(i, j) =DSkij (ESk (SK)).

**********.

[0174] In i=j when the same master key Mkj as the master key Mki used here when generating EMki (SK) is used within a decryption unit, it is Sk"(i, j) =Skij =SK. It becomes.

[0175] therefore, every -- Skij (i=1-n) -- Sk -- " (i, j) -- investigating whether =Skij (j=1-n) is materialized -- Sk -- " (i, j) -- Skij which satisfies =Skij (j=1-n) 1st session key SK ****** -- it can obtain. In addition, this Skij The thing corresponding to i to give is the master key used this time.

[0176] Now, EMki (SK) is first decoded with a master key Mkj as i= 1, for

example by the decryption circuit 112 in the key judging circuit 120 of drawing 6 , and it is Skij =DMkj (EMki (SK)).

******.

[0177] Next, it is Skij about ESk (SK) by the decryption circuit 112. It decodes and is Sk"=DSkij (ESk (SK)).

******.

[0178] next, the comparator circuit 121 -- above-mentioned Sk" and =Skij Skij or (drawing 6 (a)) Sk" (drawing 6 (b)) which compared, and controlled and held the gate circuit 122 when in agreement -- 1st session key SK ****** -- it outputs.

[0179] It is the 1st session key SK about the same actuation, making the above-mentioned i increase by every [1], when not in agreement. It repeats until it is obtained.

[0180] It is the 1st session key SK as mentioned above. After obtaining, as it mentioned above, it is the 1st session key SK at steps S20-S22. It uses and image data Data is taken out from the enciphered image data ESK (Data).

[0181] And as mentioned above, image data Data is decoded in the MPEG decoder circuit 115, is changed into an analog signal by the D/A conversion circuit 116, and is sent and reproduced by image equipments, such as television which is not illustrated.

[0182] In addition, it does not matter even if the above-mentioned step S11, step

S12, and steps S13 and S14 perform any previously in the case of this approach 2.

[0183] Moreover, the above-mentioned step S15 and step S17, and steps S16 and S18 may perform any first.

[0184] Furthermore, although n master keys (enciphered) recorded on DVD in steps S12, S16, S18, and S19 may be collectively performed in batch, you may carry out in batch for every master key of a predetermined number individual, and it is good in a line serially for every master key.

[0185] Moreover, when carrying out serially every 3rd master key, 2nd session key SK ' may be generated for every master key.

[0186] Moreover, about activation of step S20 and step S21, ESK (Data) of a predetermined number is read at the approach of performing serially in the unit of one ESK (Data), or step S20, it once stores in a buffer etc., and the approach of decoding ESK (Data) in a buffer at step S21 next or the method of performing step S20 and step S21 in pipeline processing can be considered.

[0187] Moreover, in case image data ESK (Data) is passed to the MPEG decoder circuit 115 from the decryption unit 114, you may pass in the unit of one Data and may pass in the unit of Data of a predetermined number.

[0188] According to this operation gestalt as mentioned above, it is CPU like the 1st operation gestalt. It cannot be reproduced or used even if it saves the data

which flow BUS.

[0189] Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept.

[0190] Moreover, since the 1st session key enciphered to the record medium, using two or more master keys respectively and the 1st session key enciphered for the 1st session key itself are stored according to this operation gestalt, there is an advantage of being able to use it for every predetermined unit, for example, the manufacture manufacturer of a unit, being able to assign the master key made in a decryption unit.

[0191] Moreover, the circuit used for encryption and a decryption also with this operation gestalt should just exchange decryption unit 114b (or the encryption unit 107 and decryption unit 114b), even if a code is broken, since the part used as the core of the playback part of digital recording playback devices, such as DVD, can design independently so that drawing 1 may show.

[0192] In addition, with this operation gestalt, although the code unit 107 shall have one encryption circuit, it may prepare two encryption circuits. Moreover, although decryption unit 114a shall have one decryption circuit, it may be prepared as 2, 3, 4, or five decryption circuits. It is desirable to make independent the encryption circuit and decryption circuit which correspond in these cases, or to share them by the set.

[0193] Moreover, when making independent a corresponding encryption circuit and a corresponding decryption circuit by the set, in the corresponding encryption circuit and corresponding decryption circuit which were made independent, a different cipher system from other encryption circuits and a decryption circuit may be adopted.

[0194] Next, n EMKi(s) (SK) corresponding to [like] all of i= 1 - n in DVD101 mentioned above (approach 3) are recorded, and the case where it has m Mkj(s) which make j the thing of m (<n) class of1-the n is explained in decryption unit 114a.

[0195] Since fundamental configuration, actuation, and effectiveness are the same as that of the above-mentioned approach 2, this approach 3 explains only difference here.

[0196] Although it had one master key Mkj (any one of j= 1 - the n) beforehand defined in decode unit 114a by the above-mentioned approach 2, it has the master key Mkj of m (>=2) individual beforehand defined in decode unit 114a by this approach 3. And the ranking used for the key judging mentioned above within decryption unit 114b about m master keys Mkj (any m of j= 1 - the n) is decided.

[0197] At first, they are n EMKi(s) corresponding to all of i= 1 - n in DVD101. Since (SK) is recorded, if use ranking uses the master key of the 1st place within

decryption unit 114b, it will be the 1st session key SK. Since it can obtain, it becomes the same actuation as the above-mentioned approach 2 in this case.

[0198] Next, by the approach 3, when one of master keys is torn, it supposes that use of the master key is impossible, and the case where it is made not to record EMKi (SK) corresponding to the master key it became impossible to use on DVD101 is considered henceforth.

[0199] The master key it became impossible to use here is the 1st session key SK, when use ranking is not the master key of the 1st place. Since it can obtain, it becomes the same actuation as the above-mentioned approach 2 also in this case.

[0200] Since EMKi (SK) corresponding to this master key is not recorded on DVD101 on the other hand when it becomes impossible for the master key of the 1st place to use use ranking, even if this use ranking uses the master key of the 1st place, it is the 1st session key SK at the above-mentioned step S19. It cannot obtain. In such a case, when use ranking performs the same actuation as an approach 2 within decode unit 114a using the master key of the 2nd place and this master key cannot use it, it is the 1st session key SK. It can obtain.

[0201] Even if it becomes impossible hereafter for the master key of the r-th place to use use ranking, when there are some which the r+1st place of use ranking cannot use with subsequent master keys, it is the 1st session key SK

similarly. It can obtain.

[0202] Thus, this decryption unit 114a can be used until it becomes impossible to use all the master keys of m (>=2) individual beforehand defined in decryption unit 114a.

[0203] In addition, the actuation mentioned above (approach 5) becomes being the same as that of the above (approach 3).

[0204] moreover -- having mentioned above (approach 4) -- since the information corresponding to all master keys is not stored in DVD101, when the information corresponding to the master key chosen within the decryption unit is not recorded on DVD101, it can decode like the case where the above-mentioned use is improper, the master key of the following use ranking will be chosen, and decode will be tried. therefore -- this (approach 4) -- actuation also becomes being the same as that of the above (approach 3).

[0205] By the way, it sets in this operation gestalt and is CPU. In order to encipher information and to transmit a BUS110 top to insurance, 2nd session key SK ' was used. This 2nd session key SK ' was generated within decryption unit 114a, and was told to the encryption unit 107 by the procedure using a master key. With this operation gestalt, one master key defined beforehand shall be registered into the encryption unit 107 in that case.

[0206] Instead, two or more master keys are registered also into the encryption

unit 107, and you may make it tell 2nd session key SK ' to the encryption unit 107 from decryption unit 114a using a procedure like - (approach 1) (approach 5) using a key judging mentioned above.

[0207] For example, when registering also into the encryption unit 107 the same thing as the master key registered into decryption unit 114a, it becomes the above-mentioned (approach 5).

[0208] Moreover, when registering into the encryption unit 107 some two or more things of the master key registered into decryption unit 114a, it becomes the above-mentioned (approach 3).

[0209] In addition, also when registering one master key into the encryption unit 107, the procedure of the above-mentioned (approach 2) can be used.

[0210] However, in a procedure, it becomes the procedure which replaced encryption and decode in these cases - (approach 1) (approach 5). That is, DMKi (SK) and DSK (SK) will be transmitted to the encryption unit 107 from decryption unit 114a.

[0211] in addition, 2nd session key SK ' -- CPU the configuration for telling at insurance the encryption unit 107 from decryption unit 114a through a BUS110 top -- carrying out -- the various things other than the configuration using the above-mentioned master key are applicable. For example, "Nikkei electronics The technique indicated by No.676 pp.13-14 1996.11.18" is also applicable. In

this case, registration of the master key into the encryption unit 107 is unnecessary.

[0212] (3rd operation gestalt) Next, the 3rd operation gestalt is explained.

[0213] This operation gestalt is the DVD player of a simple substance.

[0214] Drawing 9 is the block diagram showing the structure of a system concerning the 2nd operation gestalt of this invention. Moreover, an example of actuation of this operation gestalt is shown in the flow chart of drawing 10 .

[0215] This operation gestalt deletes the part about the actuation which delivers an encryption key using the 2nd session key between an encryption unit and a decode unit from the configuration of the 2nd operation gestalt.

[0216] That is, as shown in drawing 9 , the system concerning this operation gestalt is equipped with DVD driving gear (not shown) and decryption unit 114b which data read from DVD101.

[0217] Decryption unit 114b is equipped with the decryption circuit 112, the key judging circuit 120, the recovery / error correction circuit 117, and the recovery / error correction circuit 118. Moreover, with this operation gestalt, it shall have the conversion circuit 116 which changes into an analog the decoder circuit 115 and the decoded image data of MPEG from digital one in the decryption unit 114.

[0218] Here, the key judging circuit 120 is equipped with the decryption circuit 112, the comparator circuit 121, and the gate circuit 122 as shown in the

example of 1 configuration of drawing 6 .

[0219] Although three decryption circuits 112 are shown in all in decryption unit 114b in drawing 9 and drawing 6 including two decryption circuits 112 in the key judging circuit 120, it shall be one decryption circuit in fact. In addition, in the encryption unit 107, it does not have a recovery / error correction circuit 117, and the recovery / error correction circuit 118, but sides, such as a unit of the preceding paragraph, may be equipped with it.

[0220] Decryption unit 114b shall be formed as one independent IC chip.

[0221] Moreover, the master key mentioned later is registered into decryption unit 114b (made). The master key shall be recorded on the field to which the interior of a chip was kept secret so that a user could not take out intentionally in the chip of a decryption unit so that a user cannot acquire from the exterior.

[0222] SK' and the i-th thing of the master keys whose n kinds exist are expressed with Mki (it is i=1-n here), and this operation gestalt expresses [the 1st session key] image data (however, data of the enciphered bundle ball) for SK and the 2nd session key by Data. Each of these is plaintexts.

[0223] The inside of drawing 1 and 102-1 are the 1st session key SK. EMKi (SK) enciphered and generated using the master key Mki 102-2 is the 1st session key SK. 1st session key SK ESk (SK) which enciphered in person and was generated 103 is the 1st session key SK about image data Data. For 105, in

ESK (Data) used, enciphered and generated, 113 is the 1st session key SK about a master key Mkj. It expresses, respectively.

[0224] 1st session key SK recorded on DVD101 like the 2nd above-mentioned operation gestalt here EMKi enciphered and generated using the master key Mki About a setup of the number of classes of (SK), and the number of classes of a master key Mkj which it has in decryption unit 114b, as shown below, some approaches can be considered.

[0225] (Approach 1) One EMKi which makes i either1-n at DVD101 (SK) is recorded and it has n Mkj(s) corresponding to all of j= 1 - n in decryption unit 114b.

[0226] (Approach 2) n EMKi(s) (SK) corresponding to all of i= 1 - n are recorded on DVD101, and it has one Mkj which makes j either1-n in decryption unit 114b.

[0227] (Approach 3) n EMKi(s) (SK) corresponding to all of i= 1 - n are recorded on DVD101, and it has m Mkj(s) which make j the thing of m (2<m<n) class of1-the n in decryption unit 114b.

[0228] (Approach 4) m master keys EMKi (SK) which make i the thing of m (2<m<n) class beforehand chosen from that of1-the n are recorded on DVD101, and it has n master keys Mkj corresponding to all of j= 1 - n in decryption unit 114b.

[0229] (Approach 5) n master keys EMKi corresponding to all of i= 1 - n (SK) are

recorded on DVD101, and it has n master keys Mkj corresponding to all of j= 1 - n in decryption unit 114b.

[0230] As shown in drawing 3 , it is the 1st session key SK on DVD101. One piece (in the case of the above-mentioned (approach 1)) or EMKi [two or more (in the case of above-mentioned - (approach 2) (approach 5))] (SK) enciphered and generated using the master key Mki To the key record section (lead-in groove area) of a most-inner-circumference part, it is the 1st session key SK about image data Data. ESK (Data) enciphered [was used and] and generated shall be recorded on the data storage area (data area).

[0231] Next, actuation of this operation gestalt is explained, referring to the flow chart of drawing 10 . In addition, actuation of this operation gestalt deletes the part about the actuation which delivers an encryption key using the 2nd session key between an encryption unit and a decode unit from actuation of the 2nd operation gestalt.

[0232] Namely, 1st session key SK currently recorded on DVD101 by the DVD driving gear which is not illustrated at step S31 The 1st session key ESk (SK) enciphered in person is read, and it incorporates in decryption unit 114b. The error correction in a recovery and data is performed by a recovery / error correction circuit 117 in that case.

[0233] Moreover, at step S32, the 1st session key EMki (SK) which is recorded

on DVD101 by the DVD driving gear which is not illustrated and which was enciphered using the master key Mki is read, and it incorporates in decryption unit 114b. The error correction in a recovery and data is performed by a recovery / error correction circuit 117 in that case.

[0234] Next, the key judging circuit 120 is used in step S33, and it is the 1st session key SK. It asks.

[0235] The above session key [1st] SK Although the actuation for which it asks is different by (the approach 1), (an approach 2), and (an approach 3 - an approach 5), since it is the same as that of what was already explained in the 2nd operation gestalt also about which case, explanation here is omitted.

[0236] 1st session key SK After obtaining, as it mentioned above, it is steps S34-S36, and it is the 1st session key SK. It uses and image data Data is taken out from the enciphered image data ESK (Data). In addition, actuation of steps S34-S36 is CPU between units. Except that there is no delivery of image data Data through BUS, it is the same as that of steps S20-S22 (namely, steps S6-S8 already explained in the 1st operation gestalt) already explained in the 2nd operation gestalt.

[0237] And as mentioned above, image data Data is decoded in the MPEG decoder circuit 115, is changed into an analog signal by the D/A conversion circuit 116, and is sent and reproduced by image equipments, such as television

which is not illustrated.

[0238] In addition, it does not matter even if the above-mentioned step S31 and step S32 perform any previously in the case of this approach 3.

[0239] [when reaching (approaches 3-5) (approach 2)] moreover, steps S32 and S33 Although n pieces (in the case of approaches 2, 3, and 5) or m master keys (in the case of an approach 4) (enciphered) which were recorded on DVD may be collectively performed in batch, you may carry out in batch for every master key of a predetermined number individual, and it is good in a line serially for every master key.

[0240] Moreover, about activation of step S34 and step S35, ESK (Data) of a predetermined number is read at the approach of performing serially in the unit of one ESK (Data), or step S20, it once stores in a buffer etc., and the approach of decoding ESK (Data) in a buffer at step S21 next or the method of performing step S20 and step S21 in pipeline processing can be considered.

[0241] Moreover, in case image data ESK (Data) is passed to the MPEG decoder circuit 115 from the decryption unit 114, you may pass in the unit of one Data and may pass in the unit of Data of a predetermined number.

[0242] According to this operation gestalt, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept.

[0243] Moreover, according to this operation gestalt, it becomes possible to use

it suitably within limits beforehand defined on the occasion of record to DVD etc., choosing a master key. Or there is an advantage of being able to use it for every predetermined units, such as a manufacturer of a DVD player or work / selling firm of DVD, being able to assign an usable master key.

[0244] Moreover, with this operation gestalt, the circuit used for encryption and a decryption should just exchange decryption unit 114b, even if a code is broken, since the part used as the core of the playback part of digital recording playback devices, such as DVD, can design independently so that drawing 1 may show.

[0245] In addition, with this operation gestalt, although decryption unit 114b shall have one decryption circuit, it may be prepared as 2 or three decryption circuits. It is desirable to make independent the encryption circuit and decryption circuit which correspond in these cases, or to share them by the set.

[0246] Moreover, when making independent a corresponding encryption circuit and a corresponding decryption circuit by the set, in the corresponding encryption circuit and corresponding decryption circuit which were made independent, a different cipher system from other encryption circuits and a decryption circuit may be adopted.

[0247] As mentioned above, although the 1st operation gestalt, the 2nd operation gestalt (in detail three kinds of configurations), and the 3rd operation gestalt (in detail three kinds of configurations) have been explained, respectively,

this invention is not limited to these, but can deform variously and can be carried out.

[0248] With each operation gestalt, although the informational record medium was explained as a DVD, this invention is applicable to other record media, such as CD-ROM.

[0249] Although each operation gestalt explained taking the case of image data as information used as the candidate for decode, this invention can apply voice, a text, a program, etc. to the regenerative apparatus of the information on other gestalten etc.

[0250] In addition, with each operation gestalt, although Data Data were made into image data, the configuration which makes Data Data the key information Skt is also considered. That is, instead of ESK (Data), ESK (Skt) and ESkt (Data) are recorded, with the procedure shown with each operation gestalt in the decryption units 114,114a and 114b, Skt is first obtained to record media, such as DVD, ESkt (Data) is decoded by this Skt to them, and actual contents can be obtained to them. Moreover, hierarchization of such a key can be performed over the hierarchy of arbitration.

[0251] Although each operation gestalt explained taking the case of the case where the information used as the candidate for decode is compressed according to the specification of MPEG 2, this invention may not be limited to this

but a data compression or coding may be carried out by other specification. In this case, a decoder circuit [instead of the MPEG decoder circuit 115 / others] is prepared. Moreover, coding etc. may not be carried out. In this case, the MPEG decoder circuit 115 is deleted.

[0252] moreover, it is also possible to prepare two or more kinds of decoding circuits etc., to carry out change ****** of this suitably so that all of the data (or decode -- being unnecessary -- data) to which compression etc. was carried out by various methods can be outputted (or for these not to be used -- as), and to constitute. The method of reading the identifier which shows decoding which should be used from record media, such as DVD, in this case that selection etc. carries out a suitable decoding circuit etc. according to this identifier can be considered.

[0253] The configuration of the key judging circuit 120 of drawing 6 shown with the 2nd operation gestalt and the 3rd operation gestalt is an example, in addition can consider various configurations.

[0254] Furthermore, in addition to this, the configuration using ESK (SK) as information for a key judging can consider various things. DSK (SK) is used as information used for a key judging. For example, in the key judging circuit 120 Decode with the master key Mkj which had EMki (SK) read from record media, such as DVD, memorized, and Skij =DMkj (EMki (SK)) is obtained. This Skij Skij

Decode in person and Sk''' =DSkij (Skij) is obtained. Next, when DSK (SK) read from record media, such as this Sk'' and DVD, is compared and it is in agreement, it is 1st session key SK =Skij. It judges with a right thing and outputs.

[0255] Moreover, various things, such as the thing which performed encryption or decode twice or more, for example, ESK (ESK (SK)) and DSK (DSK (SK)), and a thing which prepares EMki (EMki (SK)) corresponding to each EMki (SK), can be considered as other examples of the information for a key judging.

[0256] Moreover, with each operation gestalt, although the key obtained by decode using the procedure shown by - (approach 1) (approach 5) based on the information for a key judging judged that the 1st session key was a right thing They are all EMki(s) in the sequence of i to record media, such as DVD. The information for a key judging, a key judging procedure, and the configuration for it are omissible by recording (SK), and matching and registering i and Mki into the decode unit. In addition, when it becomes impossible for Mki to use it about certain i, it is desirable to store the information which shows an invalid to record media, such as DVD, instead of EMki (SK).

[0257] Next, referring to drawing 11 , DVD-ROM is taken up for an example and the management method of the key by the key management organization which manages the 3rd above-mentioned disk manufacturer (it considers as the manufacturer who makes DVD of works, such as a movie and music) and player

manufacturer (it considers as the manufacturer of the DVD player of a simple substance) using an operation gestalt, and above-mentioned master key etc. is explained. In addition, Data may be key information as mentioned above besides contents (the explanation about the encryption using this key information Skt, decode, etc. in case Data is the key information Skt is omitted). In addition, in drawing 11 , it has omitted about the computer used for processing etc.

[0258] Moreover, drawing for explaining the system for encryption to drawing 12 is shown. It may be carried on different equipments (computer etc.) from the case where the encryption circuit 301,312,303 of drawing 12 is carried on the same equipments (computer etc.), and when it is the latter, informational delivery is performed between equipment. Moreover, the encryption circuit 301,312,303 can also be constituted [also constituting from hardware, and] from software.

[0259] Here, n master keys EMKi corresponding to all of i= 1 - n (SK) are recorded on the above-mentioned (approach 3) DVD, and the case where it has m master keys Mkj which make j the thing of m (2<m<n) class beforehand chosen from that of1-the n in a DVD player (decryption unit 114b) is explained. In addition, a master key Mkj shall be exclusively assigned to a DVD player manufacturer. Moreover, it is referred to as n= 100 and m= 10 here.

[0260] Moreover, the approach of recording ESK (SK) shall be used for DVD as

information for a key judging here (the part of 302 of drawing 12 is a thing at the time of setting information for a key judging to ESK (SK)).

[0261] First, the master key MKi (i=1-100) is kept in the key management organization 200. As for a number, it is desirable to a master key to set up too much for a player manufacturer's new comer, the reserve at the time of being broken, etc.

[0262] In the key management organization 200, a master key MKi (i=1-100) is exclusively assigned to each player manufacturers 201-203. For example, like drawing 11 , a master key MKi (i=20-29) is assigned to the player manufacturer B, and a master key MKi (i=30-39) is assigned to the player manufacturer A for a master key MKi (i=10-19) at the player manufacturer C. The assigned master keys (computer etc.) are sent with communication media or a record medium from the key management organizations 200 (computer etc.) at each player manufacturer. Delivering to insurance using cryptocommunication etc. is desirable in that case.

[0263] Each player manufacturer manages the master key assigned according to the individual from the key management organization 200. And each player manufacturer manufactures and sells the DVD player which has a configuration as shown with the 3rd operation gestalt using this assigned master key.

[0264] It is made not to, pass the plane data of a master key to the disk

manufacturers 221-223 from the key management organization 200 on the other hand here.

[0265] First, each disk manufacturer (referred to as a) is the 1st session key Sk at self. It decides (it is an arrangement for every disk), and is the 1st session key Sk. The key management organization 200 is passed. The key management organization 200 is the 1st received session key Sk. It enciphers with all the master keys MKi (i=1-100), respectively, and EMki (SK) and (i=1-100) are obtained (the encryption circuit 301 of drawing 12 is used). And the key management organization 200 hands the disk manufacturer a EMki (SK) and (i=1-100).

[0266] It is desirable for delivery of the information between the key management organization 200 and disk (calculating machine etc.) manufacturers (calculating machine etc.) as well as the above to carry out the assigned master key to insurance using cryptocommunication etc. with communication media or a record medium.

[0267] By the disk manufacturer a, EMki (SK), (i=1-100), and ESK (SK) and ESK (Data) are recorded on DVD231, and are sold. In addition, SK It is SK at self. There are an approach of performing actuation of enciphering and obtaining ESK (SK), by the disk manufacturer side, and the approach of performing by the key management organization 200 side like encryption with a master key (the

encryption circuit 312 of drawing 12 is used). Moreover, encryption at least of contents shall be performed by the disk manufacturer (the encryption circuit 303 of drawing 12 is used).

[0268] the disk manufacturer a -- SK ******** -- it manages about received EMki (SK), and ESK (SK) and ESK (Data) (or Data) which are the information for a key judging.

[0269] The same is said of other disk manufacturers.

[0270] In addition, if it should be revealed that the master key was torn, DVD is made after it, without using the torn master key. For example, when the master key of i= 19 is torn, i=1-18 and EMki (SK) corresponding to 99 of 20-100 are recorded on DVD.

[0271] Moreover, when it is revealed that the master key was torn, it is desirable after it to manufacture a DVD player except for this and to make it sell by the player manufacturer to whom the torn master key is assigned. For example, when the master key of i= 19 is torn, the player manufacturer A manufactures and sells a DVD player using the master key of i=10-18.

[0272] Moreover, about a ** DVD player with the already sold master key of i= 19, you may use it as it is. However, you may make it not have the master key of i= 19 by unit exchange etc.

[0273] Therefore, while it is effectively manageable, insurance and the risk to

unjust master key decode are distributed, and after master key decode can function a master key safely [the above-mentioned system] and effectively.

[0274] This invention is not limited to the gestalt of operation mentioned above, in the technical range, can deform variously and can be carried out.

[0275]

[Effect of the Invention] According to this invention, only a just thing with at least one of two or more 2nd keys can obtain the plane data of the data which could obtain the 1st key, therefore were enciphered with the 1st key.

[0276] Consequently, by the unjust copy, the illegal action which sells media can be prevented and copyright can be kept.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the structure of a system concerning the 1st operation gestalt of this invention

[Drawing 2] The flow chart which shows actuation of this operation gestalt

[Drawing 3] Drawing showing an example of a format which stores the data enciphered as the key enciphered by the record medium

[Drawing 4] CPU Drawing for explaining the case where data are saved from BUS

[Drawing 5] The block diagram showing the structure of a system concerning the 2nd operation gestalt of this invention

[Drawing 6] Drawing showing the example of the internal configuration of the key judging section

[Drawing 7] The flow chart which shows actuation of this operation gestalt

[Drawing 8] The flow chart which shows actuation of this operation gestalt

[Drawing 9] The block diagram showing the structure of a system concerning the 3rd operation gestalt of this invention

[Drawing 10] The flow chart which shows actuation of this operation gestalt

[Drawing 11] Drawing for explaining the management method of a key

[Drawing 12] Drawing for explaining encryption

[Description of Notations]

101 -- DVD

102,202 -- 1st session key enciphered using the master key

103,203 -- Image data enciphered using the 1st session key

104 -- Encryption circuit

105 -- Master key

106 -- 2nd session key

107 -- Encryption unit

108 -- 2nd session key decoded using the master key

109 -- 1st session key which was enciphered using the 2nd session key and which was enciphered using the master key

110 -- CPU BUS

111 -- Session key generation circuit

112 -- Decryption circuit

113 -- 1st session key

114,114a, 114b -- Decryption unit

115 -- MPEG decoder circuit

116 -- Digital to analog circuit

209 -- Line for copying to another medium from the read-out output of DVD

210 -- CPU Line for copying to another medium from BUS

211 -- Digital storage

200 -- Key management organization

201-203 -- Player manufacturer

221-223 -- Disk manufacturer

231-233 -- DVD

301,312,303 -- Encryption circuit

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－106148

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
Ｇ０９Ｃ　1/00	６３０	Ｇ０９Ｃ　1/00	６３０Ａ
			６３０Ｅ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ

審査請求　未請求　請求項の数16　ＯＬ　（全 32 頁）　最終頁に続く

(21)出願番号　特願平9－136709

(22)出願日　平成９年(1997)５月27日

(31)優先権主張番号　特願平8－170399

(32)優先日　平８(1996)６月28日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　遠藤　直樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　海野　裕明
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(74)代理人　弁理士　鈴江　武彦　（外６名）

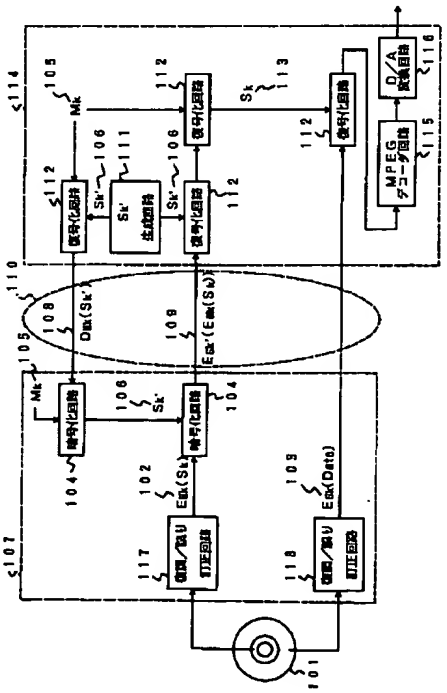
最終頁に続く

(54)【発明の名称】　暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法

(57)【要約】

【課題】　ディジタル記録された記録媒体からの不正なコピーを防止するための復号方法を提供すること。

【解決手段】　本発明に係る復号方法は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力し、前記第２の鍵の少なくとも一つを用いて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得ることを特徴とする。また、記録媒体に、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記録する。



1

【特許請求の範囲】

【請求項１】第１の鍵でデータを暗号化し、前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化することを特徴とする暗号化方法。

【請求項２】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記録したことを特徴とする記録媒体。

【請求項３】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを同一の記録媒体内に少なくとも記録することを特徴とする記録媒体の製造方法。

【請求項４】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力し、

前記第２の鍵の少なくとも一つを用いて前記第１の鍵を復号して得て、

得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項５】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力する入力手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記入力手段から入力された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする復号装置。

【請求項６】データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記読み出し手段から読み出された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする記録再生装置。

【請求項７】第１の管理者に予め定められた複数の第２の鍵を少なくとも保管させ、第２の管理者にデータを第１の鍵で暗号化した情報と前記第１の鍵を前記予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも管理させ、第３の管理者に前記第２の鍵の少なくとも１つを管理させることを特徴とする鍵の管理方法。

【請求項８】データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、

この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする復号装置。

【請求項９】記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝え、前記第２のユニットにおいて少なくとも前記データの復号を行う復号装置であって、

前記第１のユニットは、前記計算機のＣＰＵバスを介して前記第２のユニットへ、前記第１、第２および第３の情報を伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝えるための手段を備え、

前記第２のユニットは、前記計算機のＣＰＵバスを介して前記第１のユニットから、前記第１、第２および第３の情報を受け取るとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に受け取るための手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、

この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする復号装置。

【請求項１０】第３の鍵を第１の鍵で暗号化して得られ

た第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、

前記第２の鍵の少なくとも一つを記憶する記憶手段と、

前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、

この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、

この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする復号装置。

【請求項１１】前記第３の情報は、前記第１の鍵を前記第１の鍵自身で暗号化して得られた情報であり、

前記第１の復号手段は、前記記憶手段に記憶されている前記第２の鍵の一つを用いて前記第２の情報のうちの一つを復号して得られた鍵と、この鍵を用いて前記前記第３の情報を復号して得られた鍵とが一致した場合に、この鍵が正しい第１の鍵であると判定するものであることを特徴とする請求項８ないし１０のいずれか１項に記載の復号装置。

【請求項１２】前記データは、鍵情報、文書、音声、画像およびプログラムのうちの少なくとも１つを含むものであることを特徴とする請求項８ないし１１のいずれか１項に記載の復号装置。

【請求項１３】データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出し、

前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、

正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項１４】記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝え、

前記第２のユニットにて、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項１５】第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し、

前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、

正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得て、

得られた前記第３の鍵を用いて前記データを復号して得ることを特徴とする復号方法。

【請求項１６】記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続されたバス転送用ユニットから計算機のＣＰＵバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、

前記バス転送用ユニットとの間で前記計算機のＣＰＵバスを介して、少なくとも前記第２および第３の情報を外部から取得されることなく安全に受け渡しするための手

段と、
前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、
この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする復号化ユニット装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ディジタル記録されたデータに対して記録媒体からのコピーを防止するための暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法に関する。
【０００２】
【従来の技術】従来、ディジタル化された情報（例えば、文書、音声、画像、プログラムなど）を記録する媒体として、音声や画像の記録媒体ではコンパクトディスクやレーザディスクがある。また、コンピュータなどのプログラムやデータの記録媒体には、フロッピーディスクやハードディスクがある。また、これら記録媒体に加えて、大容量記録媒体であるＤＶＤ（ディジタルビデオディスク）が開発されている。
【０００３】上記のような種々のディジタル記録媒体において、記録するときにそのままのディジタルデータ（圧縮や符号化等されデコード可能なものも含む）を記録しているため、記録されたデータを他の媒体にコピーすることは、例えば音質や画質の損失なしに、かつ容易にコピーすることが可能であり、複製を大量に作り出すことができ、著作権の侵害など問題があった。
【０００４】
【発明が解決しようとする課題】上述したように、ディジタル記録媒体からコピーする場合、音質や画質の劣化がなく、マスターの音質や画質を保ったままコピーすることができる。このため、海賊版と呼ばれる不正なコピーにより、著作料を払うことなくメディアを販売する不法な行為が可能となるなどの問題があった。
【０００５】本発明は、上記事情を考慮してなされたもので、ディジタル記録された記録媒体からの不正なコピーを防止するための暗号化方法、復号方法、記録再生装置、復号装置、復号化ユニット装置、記録媒体、記録媒体の製造方法および鍵の管理方法を提供することを目的とする。
【０００６】
【課題を解決するための手段】本発明（請求項１）に係る暗号化方法は、第１の鍵でデータを暗号化し、前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化することを特徴とする。
【０００７】本発明（請求項２）に係る記録媒体は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記録したことを特徴とする。
【０００８】本発明（請求項３）に係る記録媒体の製造方法は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを同一の記録媒体内に少なくとも記録することを特徴とする。
【０００９】本発明（請求項４）に係る復号方法は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力し、前記第２の鍵の少なくとも一つを用いて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得ることを特徴とする。
【００１０】本発明（請求項５）に係る復号装置は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも入力する入力手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記入力手段から入力された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする。
【００１１】本発明（請求項６）に係る記録再生装置は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、この記憶手段内の前記第２の鍵の少なくとも一つを用いて前記読み出し手段から読み出された情報に基づいて前記第１の鍵を復号して得て、得られた第１の鍵が正しいものであることを所定の方法により判定した後に、この第１の鍵を用いて前記データを復号して得る復号手段とを備えたことを特徴とする。
【００１２】本発明（請求項７）に係る鍵の管理方法は、第１の管理者に予め定められた複数の第２の鍵を少なくとも保管させ、第２の管理者にデータを第１の鍵で暗号化した情報と前記第１の鍵を前記予め定められた複

数の第２の鍵でそれぞれ暗号化した情報とを少なくとも管理させ、第３の管理者に前記第２の鍵の少なくとも１つを管理させることを特徴とする。

【００１３】本発明によれば、複数の第２の鍵のうちの少なくとも１つを持つ正当なもののみが、第１の鍵を得ることができ、従って第１の鍵で暗号化されたデータのプレインデータを得ることができる。

【００１４】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００１５】本発明（請求項８）に係る復号装置は、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする。

【００１６】本発明（請求項９）は、記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝え、前記第２のユニットにおいて少なくとも前記データの復号を行う復号装置であって、前記第１のユニットは、前記計算機のＣＰＵバスを介して前記第２のユニットへ、前記第１、第２および第３の情報を伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝えるための手段を備え、前記第２のユニットは、前記計算機のＣＰＵバスを介して前記第１のユニットから、前記第１、第２および第３の情報を受け取るとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に受け取るための手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする。

【００１７】本発明（請求項１０）に係る復号装置は、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする。

【００１８】本発明は、記録媒体から少なくとも読み出された、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝え、前記第２のユニットにおいて少なくとも前記データの復号を行う復号装置であって、前記第１のユニットは、前記計算機のＣＰＵバスを介して前記第２のユニットへ、前記第１、第２、第３および第４の情報を伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝えるための手段を備え、前記第２のユニットは、前記計算機のＣＰＵバスを介して前記第１のユニットから、前記第１、第２、第３および第４の情報を受け取るとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に受け取るための手段と、前記第２の鍵の少なくと

も一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする。

【００１９】好ましくは、前記第３の情報は、前記第１の鍵を前記第１の鍵自身で暗号化して得られた情報であり、前記第１の復号手段は、前記記憶手段に記憶されている前記第２の鍵の一つを用いて前記第２の情報のうちの一つを復号して得られた鍵と、この鍵を用いて前記前記第３の情報を復号して得られた鍵とが一致した場合に、この鍵が正しい第１の鍵であると判定するものである。

【００２０】好ましくは、前記データは、鍵情報、文書、音声、画像およびプログラムのうちの少なくとも１つを含むものである。

【００２１】本発明（請求項１３）に係る復号方法は、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出し、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする。

【００２２】本発明（請求項１４）に係る復号方法は、記録媒体から少なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝え、前記第２のユニットにて、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記データを復号して得ることを特徴とする。

【００２３】本発明（請求項１５）に係る復号方法は、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを少なくとも記憶した記録媒体からこれら情報を少なくとも読み出す読み出し、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得て、得られた前記第３の鍵を用いて前記データを復号して得ることを特徴とする。

【００２４】本発明に係る復号方法は、記録媒体から少なくとも読み出された、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とを、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続された第１のユニットから計算機のＣＰＵバスを介して第２のユニットに伝えるとともに、少なくとも前記第２および第３の情報については、外部から取得されることなく安全に伝え、前記第２のユニットにて、前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返し、正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得て、得られた前記第３の鍵を用いて前記データを復号して得ることを特徴とする。

【００２５】本発明（請求項１６）は、記録媒体から少

なくとも読み出された、データを第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続されたバス転送用ユニットから計算機のＣＰＵバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、前記バス転送用ユニットとの間で前記計算機のＣＰＵバスを介して、少なくとも前記第２および第３の情報を外部から取得されることなく安全に受け渡しするための手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記データを復号して得る第２の復号手段とを備えたことを特徴とする。

【００２６】本発明は、記録媒体から少なくとも読み出された、第３の鍵を第１の鍵で暗号化して得られた第１の情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化して得られた第２の情報と鍵判定に用いる第３の情報とデータを前記第３の鍵で暗号化して得られた第４の情報とが、前記記録媒体の駆動装置に内蔵されたまたは前記記録媒体の駆動装置に計算機のＣＰＵバスを介さずに接続されたバス転送用ユニットから計算機のＣＰＵバスを介して伝えられ、これら情報をもとに前記データを復号する復号化ユニット装置であって、前記バス転送用ユニットとの間で前記計算機のＣＰＵバスを介して、少なくとも前記第２および第３の情報を外部から取得されることなく安全に受け渡しするための手段と、前記第２の鍵の少なくとも一つを記憶する記憶手段と、前記記憶手段に記憶されている前記第２の鍵のうちから定められた順番に従い選択した一つ用いて、前記第２の情報のうちから定められた順番に従い選択した一つの暗号化された第１の鍵を復号するとともに、少なくともこの復号結果と前記第３の情報とをもとにして、前記復号により得られたこの第１の鍵が正しいものであるか否かを判定し、正しいものと判定された第１の鍵が得られるまで前記選択および前記判定を繰り返す第１の復号手段と、この第１の復号手段により正しいものとして得られた前記第１の鍵を用いて前記第３の鍵を復号して得る第２の復号手段と、この第２の復号手段に得られた前記第３の鍵を用いて前記データを復号して得る第３の復号手段とを備えたことを特徴とする。

【００２７】本発明に係る記録媒体は、データを第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報と鍵判定に用いる情報（例えば、前記第１の鍵を前記第１の鍵自身で暗号化した情報）とを少なくとも記録したことを特徴とする。

【００２８】本発明に係る記録媒体は、第３の鍵を第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報とデータを前記第３の鍵で暗号化した情報とを少なくとも記録したことを特徴とする。

【００２９】本発明に係る記録媒体は、第３の鍵を第１の鍵で暗号化した情報と前記第１の鍵を予め定められた複数の第２の鍵でそれぞれ暗号化した情報と鍵判定に用いる情報（例えば、前記第１の鍵を前記第１の鍵自身で暗号化した情報）とデータを前記第３の鍵で暗号化した情報とを少なくとも記録したことを特徴とする。

【００３０】本発明によれば、複数の第２の鍵のうちの少なくとも１つを持つ正当なもののみが、第１の鍵を得ることができ、従って第１の鍵で暗号化されたデータのプレインデータを得ることができる。この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００３１】また、本発明によれば、暗号化ユニットと復号化ユニットとを接続する信号線に流れるデータを保存したとしても、該データは暗号化されたものであり、また、該データを暗号化するために必要な情報は、乱数をもとにして生成されるものであって、後に再現できないために、たとえ、復号ユニット内の第２の鍵（マスターキー）が破られたとしても、保存したデータを再生または利用することはできない。この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。また、本発明によれば、暗号化ユニットおよび復号化ユニットは、ディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、暗号化ユニットおよび復号化ユニットを交換するだけで良い。

【００３２】また、本発明１は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められたマスターキーで暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第２のセッションキーを生成し、生成された第２のセッションキーを前記マスターキーで復号し、復号化ユニットから暗号化ユニットへ、前記マスターキーで復号された第２のセッションキーを伝送し、暗号化ユニットにて、伝送された前記マスターキーで復号された第２のセッションキーを、前記マスターキーで暗号化して、前記第２のセッションキーを取り出

し、暗号化ユニットにて、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された第１のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを伝送し、復号化ユニットにて、伝送された前記第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記マスターキーで暗号化された第１のセッションキーを取り出し、さらに取り出された前記マスターキーで暗号化された第１のセッションキーを、前記マスターキーで復号して、前記第１のセッションキーを取り出し、取り出された前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【００３３】本発明２は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーのうちの所定のマスターキーで暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第２のセッションキーを生成し、生成された第２のセッションキーを予め定められたマスターキーで復号し、復号化ユニットから暗号化ユニットへ、前記予め定められたマスターキーで復号された第２のセッションキーを伝送し、暗号化ユニットにて、伝送された前記予め定められたマスターキーで復号された第２のセッションキーを、前記予め定められたマスターキーで暗号化して、前記第２のセッションキーを取り出し、暗号化ユニットにて、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記所定のマスターキーで暗号化された第１のセッションキーを暗号化するとともに、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキー自身で暗号化された第１のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第２のセッションキーを用いて暗号化された、前記所定のマスターキーで暗号化された第１のセッションキーを伝送するとともに、第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを伝送し、復号化ユニットにて、伝送された前記第２のセッションキーを用いて暗号化された、前記所定のマスターキーで暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記所定のマスターキーで暗号化された第１のセッションキーを取り出すとともに、伝送された前記第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記第１のセッションキー自身で暗号化された第１のセッションキーを取り出し、復号化ユニットにて、取り出された前記所定のマスターキーで暗号化された第１のセッションキーを、予め定められた複数のマスターキーのうちのいずれかで復号した第１のセッションキー候補と、取り出された前記第１のセッションキー自身で暗号化された第１のセッションキーを、該第１のセッションキー候補で復号したものとが一致した場合に、該第１のセッションキー候補を前記所定の第１のセッションキーとし、得られた前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【００３４】本発明３は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号方法であって、復号化ユニットにて、所定の乱数をもとにして第２のセッションキーを生成し、生成された第２のセッションキーを予め定められたマスターキーで復号し、復号化ユニットから暗号化ユニットへ、予め定められたマスターキーで復号された第２のセッションキーを伝送し、暗号化ユニットにて、伝送された予め定められたマスターキーで復号された第２のセッションキーを、予め定められたマスターキーで暗号化して、前記第２のセッションキーを取り出し、暗号化ユニットにて、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された第１のセッションキーを暗号化するとともに、取り出された前記第２のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキー自身で暗号化された第１のセッションキーを暗号化し、暗号化ユニットから復号化ユニットへ、第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを伝送するとともに、第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを伝送し、復号化ユニットにて、伝送された前記第２のセッションキーを用いて暗号化された、前記マスターキーで暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記マスターキーで暗号化された第１のセッションキーを取り出すとともに、伝送された前記第２のセッションキーを用いて暗号化された、前記第１のセッションキー自身で暗号化された第１のセッションキーを、前記第２のセッションキーを用いて復号し、前記第１のセッ

ションキー自身で暗号化された第１のセッションキーを取り出し、復号化ユニットにて、取り出された前記マスターキーで暗号化された第１のセッションキーを、予め定められたマスターキーで復号した第１のセッションキー候補と、取り出された前記第１のセッションキー自身で暗号化された第１のセッションキーを、該第１のセッションキー候補で復号したものとが一致した場合に、該第１のセッションキー候補を前記所定の第１のセッションキーとし、得られた前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得ることを特徴とする。

【００３５】本発明４は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの復号に用いる第１のセッションキーを得るための復号方法であって、前記マスターキーで暗号化された第１のセッションキーを、前記複数のマスターキーのうちの予め定められたものをで復号して第１のセッションキー候補を生成し、生成された前記第１のセッションキー候補を用いて、前記第１のセッションキー自身で暗号化された第１のセッションキーを復号し、前記第１のセッションキー候補と、該第１のセッションキー候補を用いて復号された、前記第１のセッションキー自身で暗号化された第１のセッションキーとを比較し、前記比較にて一致した場合に、前記第１のセッションキー候補を前記所定の第１のセッションキーとして決定することを特徴とする。

【００３６】本発明５は、上記発明１ないし３のいずれか１つの発明において、前記暗号化ユニットおよび前記復号化ユニットは、それぞれ、独立して形成された集積回路素子であることを特徴とする。

【００３７】本発明６は、上記発明１ないし３のいずれか１つの発明において、前記暗号化ユニットと前記復号化ユニットとの間で行われる伝送は、ＣＰＵ　ＢＵＳを用いて行われることを特徴とする。

【００３８】本発明７は、上記発明１ないし３のいずれか１つの発明において、前記所定の乱数は、少なくとも前記記録媒体を再生する度に変化するものであることを特徴とする。

【００３９】本発明８は、上記発明１ないし３のいずれか１つの発明において、前記所定の乱数は、所定のタイミングで得られる時間情報をもとにして生成されることを特徴とする。

【００４０】所定のタイミングは、例えば、前記記録媒体がその駆動装置に装着されたタイミングである。

【００４１】本発明９は、上記発明１ないし４のいずれか１つの発明において、前記データは、鍵情報、文書、音声、画像およびプログラムのうちの少なくとも１つを含むものであることを特徴とする。

【００４２】本発明１０は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められたマスターキーで暗号化された第１のセッションキーとを記録した記録媒体から該デジタル・データの平文を得るための復号装置であって、復号化ユニット内に設けられ、所定の条件に応じて異なる第２のセッションキーを生成する第２のセッションキー生成手段と、生成された前記第２のセッションキーを前記復号化ユニット内で前記マスターキーにて復号し、このデータを暗号化ユニット内へ伝送し、前記暗号化ユニット内で前記マスターキーで暗号化することにより前記第２のセッションキーを取り出す手段と、この手段により取り出された第２のセッションキーを用いて、前記記録媒体から読み出された前記マスターキーで暗号化された前記第１のセッションキーを暗号化し前記復号化ユニットへ伝送する手段と、この手段により復号化ユニット内へ伝送された暗号化された第１のセッションキーを前記復号化ユニット内で生成された第２のセッションキーを用いて復号した後にさらに前記マスターキーを用いて復号して前記第１のセッションキーを得る手段と、この手段により得られた前記第１のセッションキーを用いて、前記記録媒体から読み出された前記第１のセッションキーで暗号化されたデジタル・データを復号して、前記デジタル・データの平文を得る手段とを備えたことを特徴とする。

【００４３】本発明１１は、上記発明１０において、前記第２のセッションキー生成手段は、前記記録媒体の復号操作を行うごとに、あるいは時間情報に応じて異なる第２のセッションキーを生成することを特徴とする。

【００４４】本発明１２に係る記録媒体は、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録したことを特徴とする。

【００４５】記録媒体は、例えば、ＤＶＤ、ＣＤ－ＲＯＭ、フロッピーディスク、ハードディスクなど、種々のものに適用可能である。

【００４６】なお、以上の装置に係る各発明は、それぞれ、方法に係る発明や記憶媒体に係る発明としても成立し、以上の方法に係る各発明は、それぞれ、装置に係る発明や記憶媒体に係る発明としても成立する。

【００４７】本発明によれば、暗号化ユニットと復号化ユニットとを接続する信号線に流れるデータを保存したとしても、該データは暗号化されたものであり、また、該データを暗号化するために必要な情報は、乱数をもとにして生成されるものであって、後に再現できないために、たとえ、復号ユニット内のマスターキーが破られたとしても、保存したデータを再生または利用することは

できない。

【００４８】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００４９】また、本発明によれば、暗号化ユニットおよび復号化ユニットは、ディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、暗号化ユニットおよび復号化ユニットを交換するだけで良い。

【００５０】また、本発明によれば、記録媒体に、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーのうちの所定のマスターキーで暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録しておくことにより、前記所定のマスターキーが複数のマスターキーのうちのいずれであっても、複数のマスターキーを持つ復号化ユニットにより、第１のセッションキーを取り出し、この第１のセッションキーにより、データを復号することができる。

【００５１】また、本発明によれば、記録媒体に、所定の第１のセッションキーで暗号化されたデジタル・データと、予め定められた複数のマスターキーで夫々暗号化された第１のセッションキーと、第１のセッションキー自身で暗号化された第１のセッションキーとを記録しておくことにより、前記複数のマスターキーのうちのいずれかを少なくとも１つでも持つ復号化ユニットにより、第１のセッションキーを取り出し、この第１のセッションキーにより、データを復号することができる。

【００５２】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００５３】本実施形態では、あるデータａを鍵Ｋを用いて暗号化する操作をE_K（ａ）と表現し、あるデータａを鍵Ｋを用いて復号化する操作をD_K（ａ）と表現する。この表現を用いることにより、例えば、あるデータａを鍵Ｋを用いて暗号化し復号する操作は、D_K（E_K（ａ））で表される。

【００５４】また、本実施形態では、あるデータをまず復号化し、その後、復号化されたデータを暗号化してもとのデータに戻すことがある。これは、暗号の性質上、データの復号化に暗号化と同等の作用があることに基づいている。つまり、復号化したデータをもとに戻すためには復号化に用いた鍵がわからなければならず、鍵が判れば復号化したデータを暗号化することにより最初に復号化したデータが得られる。この操作は、暗号鍵をｘとしデータをｙとすれば、

$E_x(D_x(y))=y$

で表される。

【００５５】本実施形態では、ＤＶＤに記録された、ＭＰＥＧ２というデータ圧縮規格に従って圧縮され暗号化された画像データを、読み出し復号しデコードして再生するシステムを例にとって説明する。

【００５６】（第１の実施形態）以下、第１の実施形態について説明する。

【００５７】図１は、本発明の第１の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図２のフローチャートに示す。

【００５８】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機内に備えられた再生に用いるＣＰＵ（図示せず）のいわゆるＣＰＵ　ＢＵＳに接続されるものであり、暗号化されたデータ（後述するE_{SK}（Ｄａｔａ））がＣＰＵ　ＢＵＳ上を流れる構成を有するものである。なお、図１では、再生に用いるＣＰＵに関する部分のみ示している。

【００５９】図１に示すように、本実施形態に係るシステムは、ＤＶＤ１０１からデータを読み出すＤＶＤ駆動装置（図示せず）、このＤＶＤ駆動装置にＣＰＵ　ＢＵＳを介さずに接続されたまたはＤＶＤ駆動装置に内蔵された暗号化ユニット１０７、復号化ユニット１１４を備えている。

【００６０】暗号化ユニット１０７と復号化ユニット１１４は、ＣＰＵ　ＢＵＳ１１０に接続されている。復号化ユニット１１４からのデータの出力は、ＣＰＵ　ＢＵＳ以外の例えばＩ／Ｏポート等を通じて行われる。つまり、本実施形態では、データの入出力はＣＰＵ　ＢＵＳを介さずに行われるが、暗号化ユニット１０７と復号化ユニット１１４との間でのデータ転送には、ＣＰＵ　ＢＵＳが用いられる。

【００６１】暗号化ユニット１０７は、復調／誤り訂正回路１１７、復調／誤り訂正回路１１８、暗号化回路１０４を備えている。図１中で、暗号化ユニット１０７内には、２つの暗号化回路１０４を示しているが、実際には１つの暗号化回路であるものとする。暗号化ユニット１０７は、独立した１つのＩＣチップとして形成されるものとする。なお、復調／誤り訂正回路１１７および復調／誤り訂正回路１１８は、暗号化ユニット１０７内には備えず、その前段のユニット等の側（ＤＶＤ駆動装置内）に備えられる場合もある。

【００６２】一方、復号化ユニット１１４は、復号化回路１１２、第２のセッションキーS_K'を生成するセッションキー生成回路１１１を備えている。また、本実施形態では、復号化ユニット１１４内にＭＰＥＧのデコーダ回路１１５および復号された画像データをディジタルからアナログに変換する変換回路１１６を備えているものとする。図１中で、復号化ユニット１１４内には、４つの復号化回路１１２を示しているが、実際には１つの復号化回路であるものとする。復号化ユニット１１４は、独立した１つのＩＣチップとして形成されるものとする。

【００６３】また、暗号化ユニット１０７内、および復

号化ユニット１１４内には、後述するマスターキーが登録されている（作り込まれている）。マスターキーは、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【００６４】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のＣＰＵで実行することにより実現することができる。この制御部による制御の具体例としては、ＤＶＤからのデータの読み出しに関する指示、データ伝送先の指定、復号化ユニット１１４からのデータ出力に関する指示等である。また、この制御部の起動のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【００６５】本実施形態では、第１のセッションキーをS_K、第２のセッションキーをS_K'、マスターキーをM_K、画像データ（すなわち暗号化された一纏まりのデータ）をＤａｔａで表す。これらはいずれも平文である。

【００６６】図１中、１０２は第１のセッションキーS_KをマスターキーM_Kを用いて暗号化して生成された$E_{MK}(S_K)$を、１０３は画像データＤａｔａを第１のセッションキーS_Kを用いて暗号化して生成されたE_{SK}（Ｄａｔａ）を、１０５はマスターキーM_Kを、１０６は第２のセッションキーS_K'を、１０８は第２のセッションキーS_K'をマスターキーM_Kを用いて復号した$D_{MK}(S_K')$を、１０９はマスターキーM_Kを用いて暗号化された第１のセッションキー$E_{MK}(S_K)$を第２のセッションキーS_K'を用いて暗号化した$E_{SK'}(E_{MK}(S_K))$を、１１３は第１のセッションキーS_Kをそれぞれ表す。

【００６７】図３に示すように、ＤＶＤ１０１上で、第１のセッションキーS_KをマスターキーM_Kを用いて暗号化して生成された$E_{MK}(S_K)$は、最内周部分の鍵記録領域（リードインエリア）に、画像データＤａｔａを第１のセッションキーS_Kを用いて暗号化して生成されたE_{SK}（Ｄａｔａ）は、データ記録領域（データエリア）に記録されているものとする。

【００６８】以下、図２のフローチャートを参照しながら、本実施形態の動作について説明する。

【００６９】ステップＳ１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーM_Kを用いて暗号化された第１のセッションキー$E_{MK}(S_K)$を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【００７０】一方、ステップＳ２で、復号化ユニット１１４では、セッションキー生成回路１１１において、乱数、例えば時計（図示せず）からの時間情報を入力として第２のセッションキーS_K'を生成する。そして、復号化回路１１２において、生成された第２のセッションキーS_K'を、マスターキーM_Kを用いて復号して$D_{MK}(S_K')$を生成し、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【００７１】上記の乱数を発生するタイミング（例えば時間情報を入力するタイミング）としては、例えば、ＤＶＤ駆動装置にＤＶＤ１０１が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【００７２】あるいは、セッションキー生成回路１１１は、例えば鍵長分の乱数発生器で構成しても良い。なお、全てのビットが０や１になる可能性のある乱数で鍵を生成する場合は、全てのビットが０や１になることがないようにチェック処理等をする必要がある。

【００７３】ステップＳ３で、暗号ユニット１０７では、暗号化回路１０４において、ＣＰＵ　ＢＵＳ１１０を通じて受け取った$D_{MK}(S_K')$を、マスターキーM_Kを用いて暗号化する。すなわち、

$E_{MK}(D_{MK}(S_K'))=S_K'$

により、復号化ユニット１１４内のセッションキー生成回路１１１で生成された第２のセッションキーS_K'を得ることができる。

【００７４】ここで、セッションキー生成回路１１１で生成された第２のセッションキーS_K'は、ＣＰＵ　ＢＵＳ１１０上で盗まれたとしても解らないようにしてある。

【００７５】次に、ステップＳ４で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーS_K'を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキー$E_{MK}(S_K)$を暗号化して、$E_{SK'}(E_{MK}(S_K))$を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４へ送る。

【００７６】次に、ステップＳ５で、復号化ユニット１１４では、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取った$E_{SK'}(E_{MK}(S_K))$を、第２のセッションキーS_K'を用いて復号し、

$D_{SK'}(E_{SK'}(E_{MK}(S_K)))=E_{MK}(S_K)$

を得る。

【００７７】さらに、復号化回路１１２において、得られた$E_{MK}(S_K)$を、マスターキーM_Kを用いて復号し、

$D_{MK}(E_{MK}(S_K))=S_K$

となり、第１のセッションキーS_Kを得ることができる。

【００７８】以上のようにして第１のセッションキーS_Kを得た後、ステップＳ６で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーS_Kを用いて暗号化された画像データE_{SK}（Ｄａｔａ）を読み出し、暗号ユニット１０７内に取り込

む。その際、復調／誤り訂正回路１１８により復調、データ中の誤り訂正が行われる。そして、E_{SK}（Ｄａｔａ）を、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【００７９】次に、ステップＳ７で、復号化ユニット１１４では、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったE_{SK}（Ｄａｔａ）を、第１のセッションキーS_Kを用いて復号し、

D_{SK}（E_{SK}（Ｄａｔａ））＝Ｄａｔａ

となり、暗号化された画像データを復号して、平文のＤａｔａを得ることができる。

【００８０】そして、例えば復号すべきデータ（すなわちE_{SK}（Ｄａｔａ））の処理が終了し、あるいは処理の中止を要求されるまで、上記のステップＳ６とステップＳ７が繰り返し行われる。

【００８１】以上のようにして得られた画像データＤａｔａは、例えばＭＰＥＧ２というデータ圧縮規格に従って圧縮されている場合にはＭＰＥＧデコーダ回路１１５でデコードされ、そしてＤ／Ａ変換回路１１６でアナログ信号に変換された後、図示しないテレビなどの映像装置に送られ、再生される。

【００８２】なお、上記のステップＳ１と、ステップＳ２およびＳ３とは、どちらを先に実行しても構わない。

【００８３】また、ステップＳ６とステップＳ７の実行については、１つのE_{SK}（Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ６で所定数のE_{SK}（Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ７でバッファ内のE_{SK}（Ｄａｔａ）を復号する方法、あるいはステップＳ６とステップＳ７をパイプライン処理的に行う方法などが考えられる。

【００８４】また、復号化回路１１２からＭＰＥＧデコーダ回路１１５に画像データE_{SK}（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【００８５】以上のように本実施形態によれば、ディジタル化されたデータを暗号化して記録した媒体を再生する場合（暗号化されたデータを復号する場合）に、計算機のＣＰＵ　ＢＵＳに復号されたデータが流れず、また、ＣＰＵ　ＢＵＳに流れる暗号化されたデータの復号に必要な第１のセッションキーの暗号化に用いた第２のセッションキーS_K´は、例えば時間情報のようにデータ再生の度に変わる情報をもとに生成されるため、図４のようにＣＰＵ　ＢＵＳ１１０を流れるデータを信号線２１０からディジタル記憶媒体２１１に保存したとしても、それを再生または利用することはできない。

【００８６】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【００８７】また、本実施形態では、暗号化および復号化に用いる回路は、図１から解るようにＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４（あるいは暗号化ユニット１０７および復号化ユニット１１４）を交換するだけで良い。

【００８８】なお、本実施形態では、暗号ユニット１０７は１つの暗号化回路を持つものとしたが、２つの暗号化回路を設けても良い。また、復号化ユニット１１４は１つの復号化回路を持つものとしたが、２、３、または４つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【００８９】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路および復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【００９０】（第２の実施形態）次に、第２の実施形態について説明する。

【００９１】本実施形態では、例えば、予め定めた複数のマスターキーを用意し、そのうちの１つまたは複数のマスターキーを、復号化ユニットのメーカ（あるいはＤＶＤの制作・販売会社）などの所定の単位ごとに割り当てるような場合に好適な例について説明する。

【００９２】図５は、本発明の第２の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図７および図８のフローチャートに示す。

【００９３】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機内に備えられた再生に用いるＣＰＵ（図示せず）のいわゆるＣＰＵ　ＢＵＳに接続されるものであり、暗号化されたデータ（E_{SK}（Ｄａｔａ））がＣＰＵ　ＢＵＳ上を流れる構成を有するものである。なお、図５では、再生に用いるＣＰＵに関する部分のみ示している。

【００９４】図５に示すように、本実施形態に係るシステムは、ＤＶＤ１０１からデータの読み出すＤＶＤ駆動装置（図示せず）、このＤＶＤ駆動装置にＣＰＵ　ＢＵＳを介さずに接続されたまたはＤＶＤ駆動装置に内蔵された暗号化ユニット１０７、復号化ユニット１１４ａを備えている。

【００９５】暗号化ユニット１０７と復号化ユニット１１４ａは、ＣＰＵ　ＢＵＳ１１０に接続されている。復号化ユニット１１４ａからのデータの出力は、ＣＰＵ　ＢＵＳ以外の例えばＩ／Ｏポート等を通じて行われる。つまり、本実施形態では、データの入出力はＣＰＵ　ＢＵＳを介さずに行われるが、暗号化ユニット１０７と復号化ユニット１１４ａとの間でのデータ転送には、ＣＰＵ　ＢＵＳが用いられる。

【００９６】暗号化ユニット１０７は、復調／誤り訂正回路１１７、復調／誤り訂正回路１１８、暗号化回路１０４を備えている。図１中で、暗号化ユニット１０７内

には、２つの暗号化回路１０４を示しているが、実際には１つの暗号化回路であるものとする。暗号化ユニット１０７は、独立した１つのＩＣチップとして形成されるものとする。なお、復調／誤り訂正回路１１７および復調／誤り訂正回路１１８は、暗号化ユニット１０７内には備えず、その前段のユニット等の側（ＤＶＤ駆動装置内）に備えられる場合もある。

【００９７】一方、復号化ユニット１１４ａは、復号化回路１１２、第２のセッションキーS_k´を生成するセッションキー生成回路１１１、鍵判定回路１２０を備えている。

【００９８】ここで、図６に、鍵判定回路１２０の一構成例を示す。この鍵判定回路１２０は、復号化回路１１２、比較回路１２１、ゲート回路１２２を備えている。また、本実施形態では、復号化ユニット１１４ａ内にＭＰＥＧのデコーダ回路１１５および復号された画像データをディジタルからアナログに変換する変換回路１１６を備えているものとする。

【００９９】図５および図６中で、復号化ユニット１１４ａ内には、鍵判定回路１２０内の２つの復号化回路１１２を含めて、全部で５つの復号化回路１１２を示しているが、実際には１つの復号化回路であるものとする。

【０１００】復号化ユニット１１４ａは、独立した１つのＩＣチップとして形成されるものとする。

【０１０１】また、暗号化ユニット１０７内、および復号化ユニット１１４ａ内には、後述するマスターキーが登録されている（作り込まれている）。マスターキーは、利用者が外部から取得できないように、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【０１０２】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該計算機のＣＰＵで実行することにより実現することができる。この制御部による制御の具体例としては、ＤＶＤからのデータの読み出しに関する指示、データ伝送先の指定、復号化ユニット１１４ａからのデータ出力に関する指示等である。また、この制御部の起動のトリガーは、例えば、ユーザ・インタフェースを介してユーザにより行われる場合と、あるアプリケーションプログラム中のプロセスからかけられる場合などが考えられる。

【０１０３】本実施形態では、第１のセッションキーをS_k、第２のセッションキーをS_k´、ｎ種類存在するマスターキーのうちのｔ番目のものをM_{kt}（ここでｔ＝１～ｎ）、画像データ（ただし、暗号化された一纏まりのデータ）をＤａｔａで表す。これらはいずれも平文である。

【０１０４】図１中、１０２－１は第１のセッションキーS_kをマスターキーM_{ki}を用いて暗号化して生成されたE_{MKi}（S_k）を、１０２－２は第１のセッションキーS_kを第１のセッションキーS_k自身で暗号化して生成されたE_{Sk}（S_k）を、１０３は画像データＤａｔａを第１のセッションキーS_kを用いて暗号化して生成されたE_{SK}（Ｄａｔａ）を、１０５はマスターキーM_{kj}を、１０６は第２のセッションキーS_k´を、１０８は第２のセッションキーS_k´をマスターキーM_{kj}を用いて復号したD_{MKj}（S_k´）を、１０９－１はマスターキーM_{ki}を用いて暗号化された第１のセッションキーE_{MKi}（S_k）を第２のセッションキーS_k´を用いて暗号化した$E_{SK'}$（E_{MKi}（S_k））を、１０９－２は第１のセッションキーS_k自身で暗号化された第１のセッションキーE_{Sk}（S_k）を第２のセッションキーS_k´を用いて暗号化した$E_{SK'}$（E_{Sk}（S_k））を、１１３は第１のセッションキーS_kをそれぞれ表す。

【０１０５】ここで、ＤＶＤ１０１に記録する第１のセッションキーS_kをマスターキーM_{ki}を用いて暗号化して生成されたE_{MKi}（S_k）の種類数と、復号化ユニット１１４ａ内に持つマスターキーM_{kj}の種類数の設定について、例えば次に示すように幾つかの方法が考えられる。

【０１０６】（方法１）ＤＶＤ１０１にはｉを１～ｎのいずれかとする１つのマスターキーE_{MKi}（S_k）を記録し、復号化ユニット１１４ａ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーM_{kj}を備える。

【０１０７】（方法２）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーE_{MKi}（S_k）を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのいずれかとする１つのマスターキーM_{kj}を備える。

【０１０８】（方法３）上記の（方法２）を拡張したもので、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーE_{MKi}（S_k）を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーM_{kj}を備える。

【０１０９】なお、具体的な数値例としては、例えば、ｎ＝１００あるいはｎ＝４００などであり、ｍ＝２，３，あるいは４、あるいは１０などであるが、これらに限定されるものではない。

【０１１０】（方法４）上記の（方法３）においてＤＶＤと復号化ユニットを逆にした例で、ＤＶＤ１０１にはｉを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーE_{MKi}（S_k）を記録し、復号化ユニット１１４ａ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーM_{kj}を備える。

【０１１１】（方法５）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーE_{MKi}（S_k）を記録し、復号化ユニット１１４ａ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーM_{kj}を備える。

【０１１２】なお、方法３～方法５は、復号のための手

順は同様になる。

【０１１３】図３に示すように、ＤＶＤ１０１上で、第１のセッションキーS_kをマスターキーM_{ki}を用いて暗号化して生成された１個（上記の（方法１）の場合）または複数個（上記の（方法２）～（方法５）の場合）のE_{mki}（S_k）は、最内周部分の鍵記録領域（リードインエリア）に、画像データＤａｔａを第１のセッションキーS_kを用いて暗号化して生成されたE_{sk}（Ｄａｔａ）は、データ記録領域（データエリア）に記録されているものとする。

【０１１４】また、復号化ユニット１１４内に、ｎ個（上記の（方法１）、（方法４）、（方法５）の場合）、または１個（上記の（方法２）の場合）、またはｍ個（上記の（方法３）の場合）のマスターキーM_{kj}が登録されているものとする。

【０１１５】なお、暗号化ユニット１０７内には、予め定められた１つのマスターキーが登録されているものとする。

【０１１６】以下では、上記の（方法１）、（方法２）、（方法３～方法５）について順次説明する。

【０１１７】まず、上記の（方法１）の場合について図７および図８のフローチャートを参照しながら本実施形態の動作を説明する。

【０１１８】ステップＳ１１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーS_k自身で暗号化された第１のセッションキーE_{sk}（S_k）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１１９】また、ステップＳ１２で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーM_{ki}を用いて暗号化された第１のセッションキーE_{mki}（S_k）（ｉ＝１～ｎのいずれか１つ；ここではｉは未知である）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１２０】一方、ステップＳ１３で、復号化ユニット１１４ａでは、セッションキー生成回路１１１において、乱数、例えば時計（図示せず）からの時間情報を入力として第２のセッションキーS_k'を生成する。そして、復号化回路１１２において、生成された第２のセッションキーS_k'を、マスターキーM_{kj}（ここでｊは１～ｎのうち予め定められたもの）を用いて復号してD_{mkj}（S_k'）を生成し、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【０１２１】上記の乱数を発生するタイミング（例えば時間情報を入力するタイミング）としては、例えば、ＤＶＤ駆動装置にＤＶＤ１０１が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【０１２２】あるいは、セッションキー生成回路１１１は、例えば鍵長分の乱数発生器で構成しても良い。なお、全てのビットが０や１になる可能性のある乱数で鍵を生成する場合は、全てのビットが０や１になることがないようにチェック処理等をする必要がある。

【０１２３】ステップＳ１４で、暗号ユニット１０７では、暗号化回路１０４において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったD_{mkj}（S_k'）を、マスターキーM_{kj}（ここでｊは１～ｎのうち予め定められたもの）を用いて暗号化する。すなわち、

E_{mkj}（D_{mkj}（S_k'））＝S_k'

により、復号化ユニット１１４ａ内のセッションキー生成回路１１１で生成された第２のセッションキーS_k'を得ることができる。

【０１２４】ここで、セッションキー生成回路１１１で生成された第２のセッションキーS_k'は、ＣＰＵ　ＢＵＳ１１０上で盗まれたとしても解らないようにしてある。

【０１２５】次に、ステップＳ１５で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーS_k'を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキーE_{sk}（S_k）を暗号化して、E_{ssk}（E_{sk}（S_k））を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１２６】同様に、ステップＳ１６で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーS_k'を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキーE_{mki}（S_k）を暗号化して、E_{ssk}（E_{mki}（S_k））を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１２７】次に、ステップＳ１７で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったE_{ssk}（E_{sk}（S_k））を、第２のセッションキーS_k'を用いて復号し、

D_{ssk}（E_{ssk}（E_{sk}（S_k））＝E_{sk}（S_k）

を得る。

【０１２８】同様に、ステップＳ１８で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったE_{ssk}（E_{mki}（S_k））を、第２のセッションキーS_k'を用いて復号し、

D_{ssk}（E_{ssk}（E_{mki}（S_k））＝E_{mki}（S_k）

を得る。

【０１２９】ここで、E_{mki}（S_k）を生成する際に用いられたマスターキーM_{ki}は未知であるため、ステップＳ１９において、以下に示すように鍵判定回路１２０を用いて第１のセッションキーS_kを求める。

【０１３０】最初に、鍵判定処理の原理について説明する。

【０１３１】まず、E_{mki}（S_k）を、すべてのマスタ

ーキーM_{kj}（ｊ＝１～ｎ）で夫々復号すると、
S_{kij} ＝D_{mkj} （E_{mki} （S_k））（ｊ＝１～ｎ）
が得られる。ここで、S_{kij} （ｊ＝１～ｎ）のうちのいずれかが第１のセッションキーS_k である。

【０１３２】次に、上記のE_{sk}（S_k）を用いて、生成されたS_{kij} （ｊ＝１～ｎ）のいずれが第１のセッションキーS_k であるかを調べる。

【０１３３】そこで、E_{sk}（S_k）を、すべての第１のセッションキーの候補S_{kij} （ｊ＝１～ｎ）で夫々復号すると、
S_k''（ｉ，ｊ）＝D_{skij} （E_{sk}（S_k））
が得られる。

【０１３４】ここで、E_{mki} （S_k）を生成する際に用＊いられたマスターキーM_{ki} と同一のマスターキーM_{kj} を復号化ユニット内で用いた場合に、すなわち、ｉ＝ｊの場合に、S_k''（ｉ，ｊ）＝S_{kij} ＝S_k となる。

【０１３５】したがって、各S_{kij} （ｊ＝１～ｎ）について、S_k''（ｉ，ｊ）＝S_{kij} （ｊ＝１～ｎ）が成立するか否かを調べることにより、S_k''（ｉ，ｊ）＝S_{kij} （ｊ＝１～ｎ）を満足するS_{kij} を、第１のセッションキーS_k として得ることができる。なお、このS_{kij} を与えるｊに対応するものが今回使用されたマスターキーである。

【０１３６】この操作を、Ｃ言語の表記を利用してＣ言語的に表現すると、次のようになる。

```
for（i＝1；　i＜n＋1；i++）｛
　　DS1［i］＝DMK［i］（EMki（Sk））；
　　DS2［i］＝DSK［i］（Esk（Sk））；
　　if（DS1［i］＝＝DS2［i］）
　　｛
　　　　SK1＝DS2［i］；
　　　　break；
　　｝
　　else　　EXIT_MISMATCH；
｝
```

なお、上記手順の２行目は、M_{ki} を用いてE_{mi}（S_k）を復号し、これをＤＳ１［ｉ］に代入する操作を示す。

【０１３７】上記手順の３行目は、S_{ki} を用いてE_{sk}（S_k）を復号し、これをＤＳ２［ｉ］に代入する操作を示す。

【０１３８】上記手順の４行目は、ＤＳ１［ｉ］とＤＳ２［ｉ］が一致するかどうを判断する操作を示す。

【０１３９】上記手順の９行目は、ＤＳ１［ｉ］とＤＳ２［ｉ］が不一致の場合の操作を示す。

【０１４０】さて、例えば図６の鍵判定回路１２０では、復号化回路１１２により、まず、ｊ＝１として、E_{mi} （S_k）を、マスターキーM_{kj} で復号して、
S_{kij} ＝D_{mkj} （E_{mki} （S_k））
を得る。

【０１４１】次に、復号化回路１１２により、E_{sk}（S_k）をS_{kij} で復号して、
S_k''＝D_{skij} （E_{sk}（S_k））
を得る。

【０１４２】次に、比較回路１２１により、上記のS_k''と＝S_{kij} を比較し、一致した場合、ゲート回路１２２を制御して、保持しておいたS_{kij} （図６（ａ））またはS_k''（図６（ｂ））を、第１のセッションキーS_k として出力する。

【０１４３】一致しなかった場合、上記のｊを１ずつ増加させながら、同様の動作を、第１のセッションキーS_k が得られるまで繰り返す。

【０１４４】以上のようにして第１のセッションキーS_k を得た後、ステップＳ２０で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーS_k を用いて暗号化された画像データE_{sk}（Ｄａｔａ）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１８により復調、データ中の誤り訂正が行われる。そして、E_{sk}（Ｄａｔａ）を、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【０１４５】次に、ステップＳ２１で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったE_{sk}（Ｄａｔａ）を、第１のセッションキーS_k を用いて復号し、
D_{sk}（E_{sk}（Ｄａｔａ））＝Ｄａｔａ
となり、暗号化された画像データを復号して、平文のＤａｔａを得ることができる。

【０１４６】そして、例えば復号すべきデータ（すなわちE_{sk}（Ｄａｔａ））が終了し、あるいは処理の中止を要求されるまで、上記のステップＳ２０とステップＳ２１が繰り返し行われる。

【０１４７】以上のようにして得られた画像データＤａｔａは、例えばＭＰＥＧ２というデータ圧縮規格に従って圧縮されている場合にはＭＰＥＧデコーダ回路１１５でデコードされ、そしてＤ／Ａ変換回路１１６でアナログ信号に変換された後、図示しないテレビなどの映像装置に送られ、再生される。

【０１４８】なお、上記のステップＳ１１と、ステップ

Ｓ１２と、ステップＳ１３およびＳ１４とは、いずれを先に実行しても構わない。

【０１４９】また、上記のステップＳ１５およびステップＳ１７と、ステップＳ１６およびＳ１８とは、いずれを先に実行しても構わない。

【０１５０】また、ステップＳ２０とステップＳ２１の実行については、１つのE_{sk}（Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ２０で所定数のE_{sk}（Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ２１でバッファ内のE_{sk}（Ｄａｔａ）を復号する方法、あるいはステップＳ２０とステップＳ２１をパイプライン処理的に行う方法などが考えられる。

【０１５１】また、復号化回路１１２からＭＰＥＧデコーダ回路１１５に画像データE_{sk}（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【０１５２】以上のように本実施形態によれば、第１の実施形態と同様に、ＣＰＵ　ＢＵＳを流れるデータを保存したとしても、それを再生または利用することはできない。

【０１５３】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【０１５４】また、本実施形態によれば、記録媒体に記録した第１のセッションキーを暗号化するのに用いたマスターキーを直接示す情報が不要であり、ＤＶＤなどへの記録の際に予め定められた範囲内で適宜マスターキーを選択して使用することが可能となる。あるいは、ＤＶＤの制作・販売会社などの所定の単位ごとに使用可能なマスターキーを割り当てることができるなどの利点がある。

【０１５５】もちろん、本実施形態でも、暗号化および復号化に用いる回路は、ＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４ａ（あるいは暗号化ユニット１０７および復号化ユニット１１４ａ）を交換するだけで良い。

【０１５６】なお、本実施形態では、暗号化ユニット１０７は１つの暗号化回路を持つものとしたが、２つの暗号化回路を設けても良い。また、復号化ユニット１１４ａは１つの復号化回路を持つものとしたが、２、３、４、または５つの復号化回路を設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化するのが好ましい。

【０１５７】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路と復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【０１５８】次に、前述した（方法２）のように、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個の$E_{Mi}(S_k)$を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのいずれかとする１つのM_{kj}を備える場合について図７および図８のフローチャートを参照しながら本実施形態の動作を説明する。

【０１５９】ステップＳ１１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーS_k自身で暗号化された第１のセッションキー$E_{sk}(S_k)$を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１６０】また、ステップＳ１２で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーM_{ki}を用いて暗号化されたｎ個の第１のセッションキー$E_{Mki}(S_k)$（ｉ＝１～ｎ）を読み出し、暗号ユニット１０７内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０１６１】一方、ステップＳ１３で、復号化ユニット１１４ａでは、セッションキー生成回路１１１において、乱数、例えば時計（図示せず）からの時間情報を入力として第２のセッションキーS_k'を生成する。そして、復号化回路１１２において、生成された第２のセッションキーS_k'を、マスターキーM_{kj}（ここでｊは１～ｎのうち予め定められたもの）を用いて復号して$D_{Mkj}(S_k')$を生成し、ＣＰＵ　ＢＵＳ１１０を通じて暗号化ユニット１０７に送る。

【０１６２】上記の乱数を発生するタイミング（例えば時間情報を入力するタイミング）としては、例えば、ＤＶＤ駆動装置にＤＶＤ１０１が装着されたことを示す信号がアサートされたタイミングを用いることができる。

【０１６３】ステップＳ１４で、暗号ユニット１０７では、暗号化回路１０４において、ＣＰＵ　ＢＵＳ１１０を通じて受け取った$D_{Mkj}(S_k')$を、マスターキーをマスターキーM_{kj}（ここでｊは１～ｎのうち予め定められたもの）を用いて暗号化する。すなわち、

$E_{Mkj}(D_{Mkj}(S_k')) = S_k'$

により、復号化ユニット１１４ａ内のセッションキー生成回路１１１で生成された第２のセッションキーS_k'を得ることができる。

【０１６４】ここで、セッションキー生成回路１１１で生成された第２のセッションキーS_k'は、ＣＰＵ　ＢＵＳ１１０上で盗まれたとしても解らないようにしてある。

【０１６５】次に、ステップＳ１５で、暗号ユニット１０７では、上記のようにして得られた第２のセッションキーS_k'を用いて、ＤＶＤ１０１に記録された暗号化された第１のセッションキー$E_{sk}(S_k)$を暗号化して、$E_{sk'}(E_{sk}(S_k))$を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１６６】同様に、ステップＳ１６で、暗号ユニット

１０７では、上記のようにして得られた第２のセッションキーS_k'を用いて、ＤＶＤ１０１に記録された暗号化されたｎ個の第１のセッションキー$E_{Mki}(S_k)$を夫々暗号化して、$E_{SK'}(E_{Mki}(S_k))$を生成し、これをＣＰＵ　ＢＵＳ１１０を通じて復号化ユニット１１４ａへ送る。

【０１６７】次に、ステップＳ１７で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取った$E_{SK'}(E_{Sk}(S_k))$を、第２のセッションキーS_k'を用いて復号し、

$D_{SK'}(E_{SK'}(E_{Sk}(S_k)))=E_{Sk}(S_k)$

を得る。

【０１６８】同様に、ステップＳ１８で、復号化ユニット１１４ａでは、復号化回路１１２において、ＣＰＵ　ＢＵＳ１１０を通じて受け取ったｎ個の$E_{SK'}(E_{Mki}(S_k))$を、第２のセッションキーS_k'を用いて夫々復号し、

$D_{SK'}(E_{SK'}(E_{Mki}(S_k)))=E_{Mki}(S_k)$

を得る。

【０１６９】ここで、ＤＶＤ１０１に記録されているｎ個の$E_{Mki}(S_k)$（ｉ＝１～ｎ）の各々について、それを生成する際に用いられたマスターキーM_{ki}は未知であり、復号化ユニット１１４ａ内に備えられたマスターキーM_{kj}に対応するものがどれなのかは、分からないようになっている。そこで、ステップＳ１９において、以下に示すように鍵判定回路１２０を用いて第１のセッションキーS_kを求める。

【０１７０】最初に、鍵判定処理の原理について説明する。

【０１７１】まず、マスターキーM_{kj}で、すべての$E_{Mki}(S_k)$（ｉ＝１～ｎ）を夫々復号すると、

$S_{kij}=D_{Mkj}(E_{Mki}(S_k))$（ｉ＝１～ｎ）

が得られる。ここで、S_{kij}（ｉ＝１～ｎ）のうちのいずれかが第１のセッションキーS_kである。

【０１７２】次に、上記の$E_{Sk}(S_k)$を用いて、生成されたS_{kij}（ｉ＝１～ｎ）のいずれが第１のセッションキーS_kであるかを調べる。

【０１７３】そこで、$E_{Sk}(S_k)$を、すべての第１のセッションキーの候補S_{kij}（ｉ＝１～ｎ）で夫々復号すると、

$S_k''(i,j)=D_{Skij}(E_{Sk}(S_k))$

が得られる。

【０１７４】ここで、$E_{Mki}(S_k)$を生成する際に用いられたマスターキーM_{ki}と同一のマスターキーM_{kj}を復号化ユニット内で用いた場合に、すなわち、ｉ＝ｊの場合に、$S_k''(i,j)=S_{kij}=S_k$となる。

【０１７５】したがって、各S_{kij}（ｉ＝１～ｎ）について、$S_k''(i,j)=S_{kij}$（ｊ＝１～ｎ）が成立するか否かを調べることにより、$S_k''(i,j)=S_{kij}$（ｊ＝１～ｎ）を満足するS_{kij}を、第１のセッションキーS_kとして得ることができる。なお、このS_{kij}を与えるｉに対応するものが今回使用されたマスターキーである。

【０１７６】さて、例えば図６の鍵判定回路１２０では、復号化回路１１２により、まず、ｉ＝１として、$E_{Mki}(S_k)$を、マスターキーM_{kj}で復号して、

$S_{kij}=D_{Mkj}(E_{Mki}(S_k))$

を得る。

【０１７７】次に、復号化回路１１２により、$E_{Sk}(S_k)$をS_{kij}で復号して、

$S_k''=D_{Skij}(E_{Sk}(S_k))$

を得る。

【０１７８】次に、比較回路１２１により、上記のS_k''とS_{kij}を比較し、一致した場合、ゲート回路１２２を制御して、保持しておいたS_{kij}（図６（ａ））またはS_k''（図６（ｂ））を、第１のセッションキーS_kとして出力する。

【０１７９】一致しなかった場合、上記のｉを１ずつ増加させながら、同様の動作を、第１のセッションキーS_kが得られるまで繰り返す。

【０１８０】以上のようにして第１のセッションキーS_kを得た後、前述したようにステップＳ２０～Ｓ２２で、第１のセッションキーS_kを使って、暗号化された画像データE_{Sk}（Ｄａｔａ）から画像データＤａｔａを取り出す。

【０１８１】そして、前述したように、画像データＤａｔａは、ＭＰＥＧデコーダ回路１１５でデコードされ、Ｄ／Ａ変換回路１１６でアナログ信号に変換されるなどして、図示しないテレビなどの映像装置に送られ、再生される。

【０１８２】なお、この方法２の場合においても、上記のステップＳ１１と、ステップＳ１２と、ステップＳ１３およびＳ１４とは、いずれを先に実行しても構わない。

【０１８３】また、上記のステップＳ１５およびステップＳ１７と、ステップＳ１６およびＳ１８とは、いずれを先に実行しても構わない。

【０１８４】さらに、ステップＳ１２，Ｓ１６，Ｓ１８、Ｓ１９を、ＤＶＤに記録されたｎ個の（暗号化された）マスターキーを一括してバッチ的に行っても良いが、所定数個のマスターキーごとにバッチ的に行っても良いし、１つのマスターキーごとに逐次行っても良い。

【０１８５】また、３番目の１つのマスターキーごとに逐次行う場合、第２のセッションキーS_k'を、マスターキーごとに生成しても良い。

【０１８６】また、ステップＳ２０とステップＳ２１の実行については、１つのE_{Sk}（Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ２０で所定数のE_{Sk}（Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ２１でバッファ内のE_{Sk}（Ｄａｔａ）を復号

する方法、あるいはステップＳ２０とステップＳ２１をパイプライン処理的に行う方法などが考えられる。

【０１８７】また、復号化ユニット１１４からＭＰＥＧデコーダ回路１１５に画像データE_{sk}（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【０１８８】以上のように本実施形態によれば、第１の実施形態と同様に、ＣＰＵ　ＢＵＳを流れるデータを保存したとしても、それを再生または利用することはできない。

【０１８９】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【０１９０】また、本実施形態によれば、記録媒体に複数のマスターキーを夫々用いて暗号化した第１のセッションキーと、第１のセッションキー自身で暗号化した第１のセッションキーとを格納するので、復号化ユニット内に作り込むマスターキーを、所定の単位、例えばユニットの製造メーカーごとに割り当てて使用することができるなどの利点がある。

【０１９１】また、本実施形態でも、暗号化および復号化に用いる回路は、図１から解るようにＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４ｂ（あるいは暗号化ユニット１０７および復号化ユニット１１４ｂ）を交換するだけで良い。

【０１９２】なお、本実施形態では、暗号ユニット１０７は１つの暗号化回路を持つものとしたが、２つの暗号化回路を設けても良い。また、復号化ユニット１１４ａは１つの復号化回路を持つものとしたが、２、３、４、または５つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【０１９３】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路と復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【０１９４】次に、前述した（方法３）のように、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のE_{wki}（S_k）を記録し、復号化ユニット１１４ａ内にはｊを１～ｎのうちのｍ（＜ｎ）種類のものとするｍ個のM_{kj}を備える場合について説明する。

【０１９５】この方法３は、基本的な構成・動作・効果は上記の方法２と同様であるので、ここでは、相違点のみを説明する。

【０１９６】上記の方法２では、復号ユニット１１４ａ内に予め定めた１個のマスターキーM_{kj}（ｊ＝１～ｎのいずれか１つ）を備えたが、この方法３では、復号ユニット１１４ａ内に予め定めたｍ（≧２）個のマスターキーM_{kj}を備えておく。そして、ｍ個のマスターキーM_{kj}（ｊ＝１～ｎのいずれかｍ個）について、復号化ユニット１１４ｂ内で前述した鍵判定に使用する順位を決めておく。

【０１９７】最初は、ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のE_{wki}（S_k）を記録しているので、復号化ユニット１１４ｂ内で使用順位が１位のマスターキーを用いれば、第１のセッションキーS_kを得ることができるので、この場合には、前述の方法２と同様の動作になる。

【０１９８】次に、方法３では、いずれかのマスターキーが破られるなどした場合、そのマスターキーを使用不可とし、以降、ＤＶＤ１０１には使用不可となったマスターキーに対応するE_{wki}（S_k）を記録しないようにした場合を考える。

【０１９９】ここで、使用不可となったマスターキーが、使用順位が１位のマスターキーでない場合、第１のセッションキーS_kを得ることができるので、この場合にも、前述の方法２と同様の動作になる。

【０２００】一方、使用順位が１位のマスターキーが使用不可となった場合、ＤＶＤ１０１に該マスターキーに対応するE_{wki}（S_k）は記録されていないので、この使用順位が１位のマスターキーを使っても、前述のステップＳ１９にて第１のセッションキーS_kを得ることはできない。このような場合に、復号ユニット１１４ａ内で、使用順位が２位のマスターキーを用いて方法２と同様の動作を行うことにより、このマスターキーが使用不可となっていない場合、第１のセッションキーS_kを得ることができる。

【０２０１】以下、使用順位がｒ位のマスターキーが使用不可となっても、使用順位がｒ＋１位以降のマスターキーで使用不可となっていないものがある場合、同様にして第１のセッションキーS_kを得ることができる。

【０２０２】このようにして、復号化ユニット１１４ａ内に予め定めたｍ（≧２）個のマスターキーが全て使用不可となるまで、本復号化ユニット１１４ａを使用することができる。

【０２０３】なお、前述した（方法５）の動作は、上記（方法３）と同様になる。

【０２０４】また、前述した（方法４）は、ＤＶＤ１０１には全てのマスターキーに対応する情報が格納されていないので、復号化ユニット内で選択したマスターキーに対応する情報がＤＶＤ１０１に記録されていない場合には、上記の使用不可の場合と同様に復号できないことになり、次の使用順位のマスターキーを選択して復号を試行することになる。従って、この（方法４）の動作も、上記（方法３）と同様になる。

【０２０５】ところで、本実施形態において、ＣＰＵ　ＢＵＳ１１０上を情報を暗号化して安全に転送するために、第２のセッションキーS_k´を用いた。この第２の

セッションキーS_k´は、復号化ユニット114a内で生成され、マスターキーを用いた手順により暗号化ユニット107に伝えられた。その際、本実施形態では、暗号化ユニット107内には、予め定められた1つのマスターキーが登録されているものとした。

【0206】その代わりに、暗号化ユニット107内にも複数のマスター鍵を登録しておき、鍵判定を用いる前述した（方法1）～（方法5）のような手順を用いて、第2のセッションキーS_k´を復号化ユニット114aから暗号化ユニット107に伝えるようにしてもよい。

【0207】例えば、復号化ユニット114a内に登録されているマスターキーと同一のものを暗号化ユニット107にも登録する場合、上記の（方法5）になる。

【0208】また、復号化ユニット114a内に登録されているマスターキーの一部の複数のものを暗号化ユニット107に登録する場合、上記の（方法3）になる。

【0209】なお、暗号化ユニット107に1つのマスターキーを登録する場合にも、上記の（方法2）の手順を用いることができる。

【0210】ただし、これらの場合、（方法1）～（方法5）の手順において、暗号化と復号とを入れ替えた手順となる。すなわち、復号化ユニット114aから暗号化ユニット107にD_{Mki}（S_k）とD_{Sk}（S_k）とを転送することになる。

【0211】なお、第2のセッションキーS_k´をCPU BUS110上を介して復号化ユニット114aから暗号化ユニット107に安全に伝えるための構成としは、上記のマスターキーを用いる構成の他にも、種々のものが適用可能である。例えば、「日経エレクトロニクス No. 676 pp. 13－14 1996. 11. 18」に開示された技術を応用することもできる。この場合、暗号化ユニット107内へのマスターキーの登録は不要である。

【0212】（第3の実施形態）次に、第3の実施形態について説明する。

【0213】本実施形態は、例えば単体のDVDプレーヤーである。

【0214】図9は、本発明の第2の実施形態に係るシステムの構成を示すブロック図である。また、本実施形態の動作の一例を図10のフローチャートに示す。

【0215】本実施形態は、第2の実施形態の構成から、暗号化ユニットと復号ユニットとの間で第2のセッションキーを用いて暗号化鍵を受け渡しする動作に関する部分を削除したものである。

【0216】すなわち、図9に示すように、本実施形態に係るシステムは、DVD101からデータの読み出すDVD駆動装置（図示せず）、復号化ユニット114bを備えている。

【0217】復号化ユニット114bは、復号化回路112、鍵判定回路120、復調／誤り訂正回路117、復調／誤り訂正回路118を備えている。また、本実施形態では、復号化ユニット114内にMPEGのデコーダ回路115および復号された画像データをディジタルからアナログに変換する変換回路116を備えているものとする。

【0218】ここで、鍵判定回路120は、図6の一構成例に示すように、復号化回路112、比較回路121、ゲート回路122を備えている。

【0219】図9および図6中で、復号化ユニット114b内には、鍵判定回路120内の2つの復号化回路112を含めて、全部で3つの復号化回路112を示しているが、実際には1つの復号化回路であるものとする。なお、復調／誤り訂正回路117および復調／誤り訂正回路118は、暗号化ユニット107内には備えず、その前段のユニット等の側に備えられる場合もある。

【0220】復号化ユニット114bは、独立した1つのICチップとして形成されるものとする。

【0221】また、復号化ユニット114b内には、後述するマスターキーが登録されている（作り込まれている）。マスターキーは、利用者が外部から取得できないように、復号化ユニットのチップにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【0222】本実施形態では、第1のセッションキーをS_k、第2のセッションキーをS_k´、n種類存在するマスターキーのうちのi番目のものをM_{ki}（ここでi＝1～n）、画像データ（ただし、暗号化された一纏まりのデータ）をDataで表す。これらはいずれも平文である。

【0223】図1中、102－1は第1のセッションキーS_kをマスターキーM_{ki}を用いて暗号化して生成されたE_{Mki}（S_k）を、102－2は第1のセッションキーS_kを第1のセッションキーS_k自身で暗号化して生成されたE_{Sk}（S_k）を、103は画像データDataを第1のセッションキーS_kを用いて暗号化して生成されたE_{Sk}（Data）を、105はマスターキーM_{kj}を、113は第1のセッションキーS_kをそれぞれ表す。

【0224】ここで、前述の第2の実施形態と同様に、DVD101に記録する第1のセッションキーS_kをマスターキーM_{ki}を用いて暗号化して生成されたE_{Mki}（S_k）の種類数と、復号化ユニット114b内に持つマスターキーM_{kj}の種類数の設定について、例えば次に示すように幾つかの方法が考えられる。

【0225】（方法1）DVD101にはiを1～nのいずれかとする1つのE_{Mki}（S_k）を記録し、復号化ユニット114b内にはj＝1～nのすべてに対応するn個のM_{kj}を備える。

【0226】（方法2）DVD101にはi＝1～nのすべてに対応するn個のE_{Mki}（S_k）を記録し、復号

化ユニット１１４ｂ内にはｊを１～ｎのいずれかとする１つのM_{kj}を備える。

【０２２７】（方法３）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のE_{mki}（S_k）を記録し、復号化ユニット１１４ｂ内にはｊを１～ｎのうちのｍ（２＜ｍ＜ｎ）種類のものとするｍ個のM_{kj}を備える。

【０２２８】（方法４）ＤＶＤ１０１にはｉを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーE_{mki}（S_k）を記録し、復号化ユニット１１４ｂ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーM_{kj}を備える。

【０２２９】（方法５）ＤＶＤ１０１にはｉ＝１～ｎのすべてに対応するｎ個のマスターキーE_{mki}（S_k）を記録し、復号化ユニット１１４ｂ内にはｊ＝１～ｎのすべてに対応するｎ個のマスターキーM_{kj}を備える。

【０２３０】図３に示すように、ＤＶＤ１０１上で、第１のセッションキーS_kをマスターキーM_{ki}を用いて暗号化して生成された１個（上記の（方法１）の場合）または複数個（上記の（方法２）～（方法５）の場合）のE_{mki}（S_k）は、最内周部分の鍵記録領域（リードインエリア）に、画像データＤａｔａを第１のセッションキーS_kを用いて暗号化して生成されたE_{sk}（Ｄａｔａ）は、データ記録領域（データエリア）に記録されているものとする。

【０２３１】次に、図１０のフローチャートを参照しながら本実施形態の動作について説明する。なお、本実施形態の動作は、第２の実施形態の動作から、暗号化ユニットと復号ユニットとの間で第２のセッションキーを用いて暗号化鍵を受け渡しする動作に関する部分を削除したものである。

【０２３２】すなわち、ステップＳ３１で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、第１のセッションキーS_k自身で暗号化された第１のセッションキーE_{sk}（S_k）を読み出し、復号化ユニット１１４ｂ内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０２３３】また、ステップＳ３２で、図示しないＤＶＤ駆動装置によりＤＶＤ１０１に記録されている、マスターキーM_{ki}を用いて暗号化された第１のセッションキーE_{mki}（S_k）を読み出し、復号化ユニット１１４ｂ内に取り込む。その際、復調／誤り訂正回路１１７により復調、データ中の誤り訂正が行われる。

【０２３４】次に、ステップＳ３３において、鍵判定回路１２０を用いて第１のセッションキーS_kを求める。

【０２３５】以上の第１のセッションキーS_kを求める動作は、（方法１）、（方法２）、（方法３～方法５）により相違するが、いずれの場合についても既に第２の実施形態において説明したものと同様であるので、ここでの説明は省略する。

【０２３６】第１のセッションキーS_kを得た後は、前述したようにステップＳ３４～Ｓ３６で、第１のセッションキーS_kを使って、暗号化された画像データE_{sk}（Ｄａｔａ）から画像データＤａｔａを取り出す。なお、ステップＳ３４～Ｓ３６の動作は、ユニット間でＣＰＵ　ＢＵＳを介した画像データＤａｔａの受け渡しがない以外は、第２の実施形態において既に説明したステップＳ２０～Ｓ２２（すなわち、第１の実施形態において既に説明したステップＳ６～Ｓ８）と同様である。

【０２３７】そして、前述したように、画像データＤａｔａは、ＭＰＥＧデコーダ回路１１５でデコードされ、Ｄ／Ａ変換回路１１６でアナログ信号に変換されるなどして、図示しないテレビなどの映像装置に送られ、再生される。

【０２３８】なお、この方法３の場合においても、上記のステップＳ３１と、ステップＳ３２とは、いずれを先に実行しても構わない。

【０２３９】また、（方法２）および（方法３～５）の場合において、ステップＳ３２、Ｓ３３を、ＤＶＤに記録されたｎ個（方法２，３，５の場合）あるいはｍ個（方法４の場合）の（暗号化された）マスターキーを一括してバッチ的に行っても良いが、所定数個のマスターキーごとにバッチ的に行っても良いし、１つのマスターキーごとに逐次行っても良い。

【０２４０】また、ステップＳ３４とステップＳ３５の実行については、１つのE_{sk}（Ｄａｔａ）の単位で逐次行う方法、あるいはステップＳ２０で所定数のE_{sk}（Ｄａｔａ）を読み込み、一旦バッファなどへ格納し、次にステップＳ２１でバッファ内のE_{sk}（Ｄａｔａ）を復号する方法、あるいはステップＳ２０とステップＳ２１をパイプライン処理的に行う方法などが考えられる。

【０２４１】また、復号化ユニット１１４からＭＰＥＧデコーダ回路１１５に画像データE_{sk}（Ｄａｔａ）を渡す際に、１つのＤａｔａの単位で渡しても良いし、所定数のＤａｔａの単位で渡しても良い。

【０２４２】本実施形態によれば、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【０２４３】また、本実施形態によれば、ＤＶＤなどへの記録の際に予め定められた範囲内で適宜マスターキーを選択して使用することが可能となる。あるいは、ＤＶＤプレーヤーのメーカまたはＤＶＤの制作・販売会社などの所定の単位ごとに使用可能なマスターキーを割り当てて使用することができるなどの利点がある。

【０２４４】また、本実施形態では、暗号化および復号化に用いる回路は、図１から解るようにＤＶＤなどのディジタル記録再生機器の再生部分のコアとなる個所とは別に設計できるため、たとえ暗号が破られたとしても、復号化ユニット１１４ｂを交換するだけで良い。

【０２４５】なお、本実施形態では、復号化ユニット１１４ｂは１つの復号化回路を持つものとしたが、２また

は３つの復号化回路として設けても良い。これらの場合、対応する暗号化回路と復号化回路をセットで独立化しあるいは共用するのが好ましい。

【０２４６】また、対応する暗号化回路と復号化回路をセットで独立化する場合、独立化した対応する暗号化回路および復号化回路では、他の暗号化回路および復号化回路とは異なる暗号方式を採用しても構わない。

【０２４７】以上、第１の実施形態、第２の実施形態（より詳しくは３種類の構成）、第３の実施形態（より詳しくは３種類の構成）について夫々説明してきたが、本発明はこれらに限定されず種々変形して実施することができる。

【０２４８】各実施形態では、情報の記録媒体をＤＶＤとして説明したが、本発明は、ＣＤ－ＲＯＭ等他の記録媒体にも適用可能である。

【０２４９】各実施形態では、復号対象となる情報として画像データを例にとって説明したが、本発明は、音声、テキスト、プログラムなど、他の形態の情報の再生装置等にも適用可能である。

【０２５０】なお、各実施形態では、データＤａｔａを画像データとしたが、データＤａｔａを鍵情報S_{kt}とする構成も考えられる。すなわち、ＤＶＤ等の記録媒体に、E_{SK}（Ｄａｔａ）の代わりに、E_{SK}（S_{kt}）とE_{Skt}（Ｄａｔａ）を記録しておき、復号化ユニット１１４，１１４ａ，１１４ｂにおいて各実施形態で示した手順により、まずS_{kt}を得て、このS_{kt}でE_{Skt}（Ｄａｔａ）を復号して実際のコンテンツを得るようにすることもできる。また、このような鍵の階層化は、任意の階層に渡って行うことができる。

【０２５１】各実施形態では、復号対象となる情報がＭＰＥＧ２という規格に従って圧縮されている場合を例にとって説明したが、本発明はこれに限定されず、他の規格によってデータ圧縮あるいは符号化等されていても構わない。この場合、ＭＰＥＧデコーダ回路１１５の代わりに、他の対応するデコーダ回路を設ける。また、符号化等されていないものであっても構わない。この場合、ＭＰＥＧデコーダ回路１１５を削除する。

【０２５２】また、種々の方式で圧縮等されたデータ（あるいは復号の必要ないデータ）のいずれも出力できるように、複数種類のデコード回路等を設け、これを適宜切替て使用し（あるいはこれらを使用しないように）構成することも可能である。この場合、例えば、ＤＶＤ等の記録媒体から使用すべきデコード等を示す識別子を読み込む、この識別子に従って適切なデコード回路等を選択等する方法が考えられる。

【０２５３】第２の実施形態および第３の実施形態にて示した図６の鍵判定回路１２０の構成は一例であり、この他にも種々の構成が考えられる。

【０２５４】さらに、鍵判定用情報としてE_{SK}（S_K）を用いる構成は、この他にも種々のものが考えられる。例えば、鍵判定に用いる情報としてD_{SK}（S_K）を用い、鍵判定回路１２０では、ＤＶＤ等の記録媒体から読み込んだE_{Mkj}（S_K）を記憶されたマスターキーM_{kj}で復号してS_{kkj}＝D_{Mkj}（E_{Mkj}（S_K））を得て、このS_{kkj}をS_{kkj}自身で復号してS_K'''＝D_{Skkj}（S_{kkj}）を得て、次に、このS_K''とＤＶＤ等の記録媒体から読み込んだD_{SK}（S_K）を比較し、一致した場合、第１のセッションキーS_K＝S_{kkj}は正しいものと判定して出力する。

【０２５５】また、鍵判定用情報の他の例として、２回以上暗号化または復号を行ったもの、例えば、E_{SK}（E_{SK}（S_K））、D_{SK}（D_{SK}（S_K））、あるいは各E_{Mki}（S_K）に対応してE_{Mki}（E_{Mki}（S_K））を設けるものなど種々のものが考えられる。

【０２５６】また、各実施形態では、鍵判定用情報をもとに（方法１）～（方法５）で示した手順を用いて、復号により得られた鍵が第１のセッションキーが正しいものであることを判定したが、ＤＶＤ等の記録媒体にｉの順番ですべてのE_{Mki}（S_K）を記録しておき、復号ユニットにはｉとM_{ki}を対応付けて登録しておくことにより、鍵判定用情報、鍵判定手順、そのための構成を省略することができる。なお、あるｉについてのM_{ki}が使用不可となった場合には、ＤＶＤ等の記録媒体にE_{Mki}（S_K）の代わりに無効を示す情報を格納するのが望ましい。

【０２５７】次に、図１１を参照しながら、ＤＶＤ－ＲＯＭを例に取り上げ、上記した第３の実施形態を用いたディスクメーカ（映画、音楽等の著作物のＤＶＤを制作するメーカとする）とプレーヤメーカ（単体のＤＶＤプレーヤのメーカとする）とマスターキーを管理する鍵管理組織による鍵の管理方法等について説明する。なお、Ｄａｔａは、コンテンツの他に、前述したように鍵情報である場合もある（Ｄａｔａが鍵情報S_{kt}である場合のこの鍵情報S_{kt}を用いた暗号化や復号等についての説明は省略する）。なお、図１１において、処理等に用いる計算機等については省略してある。

【０２５８】また、図１２には暗号化のためのシステムに関して説明するための図を示す。図１２の暗号化回路３０１，３１２，３０３は、同一の装置（計算機等）上に搭載される場合と、異なる装置（計算機等）上に搭載される場合があり、後者の場合には、装置間で情報の受け渡しが行われる。また、暗号化回路３０１，３１２，３０３は、ハードウェアで構成することも、ソフトウェアで構成することも可能である。

【０２５９】ここでは、上記した（方法３）のＤＶＤにはｉ＝１～ｎのすべてに対応するｎ個のマスターキーE_{Mki}（S_K）を記録し、ＤＶＤプレーヤ（復号化ユニット１１４ｂ）内にはｊを１～ｎのうちのから予め選択されたｍ（２＜ｍ＜ｎ）種類のものとするｍ個のマスターキーM_{kj}を備える場合について説明する。なお、ＤＶＤ

プレーヤメーカにはマスターキーM_{kj}を排他的に割り当てるものとする。また、ここでは、ｎ＝１００、ｍ＝１０とする。

【０２６０】また、ここでは、鍵判定用情報として、ＤＶＤにはE_{sk}（S_k）を記録する方法を用いるものとする（図１２の３０２の部分は、鍵判定用情報をE_{sk}（S_k）とした場合のものである）。

【０２６１】まず、鍵管理組織２００では、マスターキーM_{ki}（ｉ＝１～１００）を保管している。マスターキーに数は、プレーヤメーカの新規参入や破られた場合の予備等のために、余分に設定しておくのが望ましい。

【０２６２】鍵管理組織２００では、各プレーヤメーカ２０１～２０３に、排他的にマスターキーM_{ki}（ｉ＝１～１００）を割り当てる。例えば、図１１のように、プレーヤメーカＡにマスターキーM_{ki}（ｉ＝１０～１９）を、プレーヤメーカＢにマスターキーM_{ki}（ｉ＝２０～２９）を、プレーヤメーカＣにマスターキーM_{ki}（ｉ＝３０～３９）を割り当てる。鍵管理組織２００（の計算機等）から各プレーヤメーカ（の計算機等）には、割り当てたマスターキーを通信媒体あるいは記録媒体等により送付する。その際、暗号通信等を用いて安全に受け渡しするのが望ましい。

【０２６３】各プレーヤメーカは、個別に、鍵管理組織２００から割り当てられたマスターキーを管理する。そして、各プレーヤメーカは、この割り当てられたマスターキーを用いて、第３の実施形態で示したような構成を有するＤＶＤプレーヤを製造して販売する。

【０２６４】一方、ここでは、鍵管理組織２００からディスクメーカ２２１～２２３へは、マスターキーのプレインデータは渡さないようにするものとする。

【０２６５】まず、各ディスクメーカ（ａとする）は、自身で第１のセッションキーS_kを決め（例えばディスク毎に決め）、第１のセッションキーS_kを鍵管理組織２００に渡す。鍵管理組織２００は、受け取った第１のセッションキーS_kを全てのマスターキーM_{ki}（ｉ＝１～１００）でそれぞれ暗号化してE_{mki}（S_k）、（ｉ＝１～１００）を得る（図１２の暗号化回路３０１を用いる）。そして、鍵管理組織２００は、E_{mki}（S_k）、（ｉ＝１～１００）を、ディスクメーカａに渡す。

【０２６６】鍵管理組織２００（の計算機等）とディスクメーカ（の計算機等）との間での情報の受け渡しも、上記と同様に、割り当てたマスターキーを通信媒体あるいは記録媒体等にて暗号通信等を用いて安全に行うのが望ましい。

【０２６７】ディスクメーカａでは、E_{mki}（S_k）、（ｉ＝１～１００）と、E_{sk}（S_k）と、E_{sk}（Ｄａｔａ））とをＤＶＤ２３１に記録して販売する。なお、S_k自身でS_kを暗号化してE_{sk}（S_k）を得る操作は、ディスクメーカ側で行う方法と、マスターキーによる暗号化と同様に鍵管理組織２００側で行う方法とがある（図１２の暗号化回路３１２を用いる）。また、少なくとも、コンテンツの暗号化はディスクメーカにて行うものとする（図１２の暗号化回路３０３を用いる）。

【０２６８】ディスクメーカａでは、例えば、S_kについて、受け取ったE_{mki}（S_k）と鍵判定用情報であるE_{sk}（S_k）とE_{sk}（Ｄａｔａ）（あるいはＤａｔａ）について管理する。

【０２６９】他のディスクメーカについても同様である。

【０２７０】なお、万一、マスターキーが破られたことが発覚した場合、それ以降、その破られたマスターキーを用いずに、ＤＶＤを制作するようにする。例えば、ｉ＝１９のマスターキーが破られた場合、ＤＶＤには、ｉ＝１～１８、２０～１００の９９個に対応するE_{mki}（S_k）が記録される。

【０２７１】また、マスターキーが破られたことが発覚した場合、それ以降、その破られたマスターキーが割り当てられているプレーヤメーカでは、これを除いてＤＶＤプレーヤを製造して販売するようにするのが望ましい。例えば、ｉ＝１９のマスターキーが破られた場合、プレーヤメーカＡは、ｉ＝１０～１８のマスターキーを用いてＤＶＤプレーヤを製造して販売する。

【０２７２】また、既に販売されたｉ＝１９のマスターキーを持つてＤＶＤプレーヤについては、そのまま使用しても構わない。ただし、ユニット交換等によってｉ＝１９のマスターキーを持たないようにしてもよい。

【０２７３】従って、マスターキーを安全かつ有効に管理できるとともに、不正なマスターキー解読に対するリスクを分散し、マスターキー解読後も上記システムが安全かつ有効に機能するようにすることができる。

【０２７４】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０２７５】

【発明の効果】本発明によれば、複数の第２の鍵のうちの少なくとも１つを持つ正当なもののみが、第１の鍵を得ることができ、従って第１の鍵で暗号化されたデータのプレインデータを得ることができる。

【０２７６】この結果、不正なコピーにより、メディアを販売する不法な行為を防止し、著作権を守ることができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るシステムの構成を示すブロック図

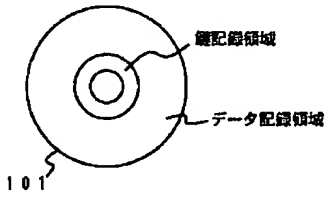
【図２】同実施形態の動作を示すフローチャート

【図３】記録媒体に暗号化された鍵と暗号化されたデータを格納する形式の一例を示す図

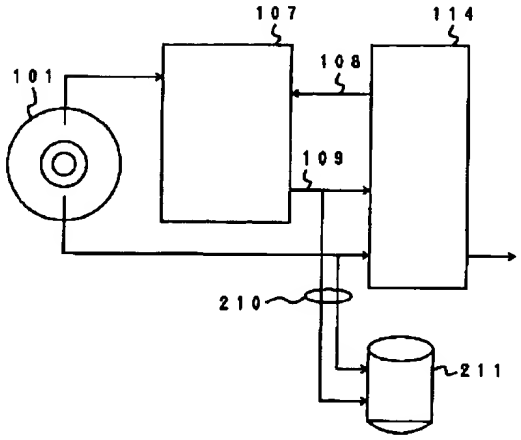
【図４】ＣＰＵ　ＢＵＳからデータを保存した場合について説明するための図

【図５】本発明の第２の実施形態に係るシステムの構成を示すブロック図
【図６】鍵判定部の内部構成の例を示す図
【図７】同実施形態の動作を示すフローチャート
【図８】同実施形態の動作を示すフローチャート
【図９】本発明の第３の実施形態に係るシステムの構成を示すブロック図
【図１０】同実施形態の動作を示すフローチャート
【図１１】鍵の管理方法について説明するための図
【図１２】暗号化について説明するための図
【符号の説明】
１０１…ＤＶＤ
１０２，２０２…マスターキーを用いて暗号化された第１のセッションキー
１０３，２０３…第１のセッションキーを用いて暗号化された画像データ
１０４…暗号化回路
１０５…マスターキー
１０６…第２のセッションキー
１０７…暗号化ユニット
１０８…マスターキーを用いて復号された第２のセッション＊キー
１０９…第２のセッションキーを用いて暗号化された、マスターキーを用いて暗号化された第１のセッションキー
１１０…ＣＰＵ　ＢＵＳ
１１１…セッションキー生成回路
１１２…復号化回路
１１３…第１のセッションキー
１１４，１１４ａ，１１４ｂ…復号化ユニット
１１５…ＭＰＥＧデコーダ回路
１１６…ディジタル／アナログ変換回路
２０９…ＤＶＤの読み出し出力から別の媒体にコピーするための線
２１０…ＣＰＵ　ＢＵＳから別の媒体にコピーするための線
２１１…ディジタル記憶媒体
２００…鍵管理組織
２０１～２０３…プレーヤメーカ
２２１～２２３…ディスクメーカ
２３１～２３３…ＤＶＤ
３０１，３１２，３０３…暗号化回路

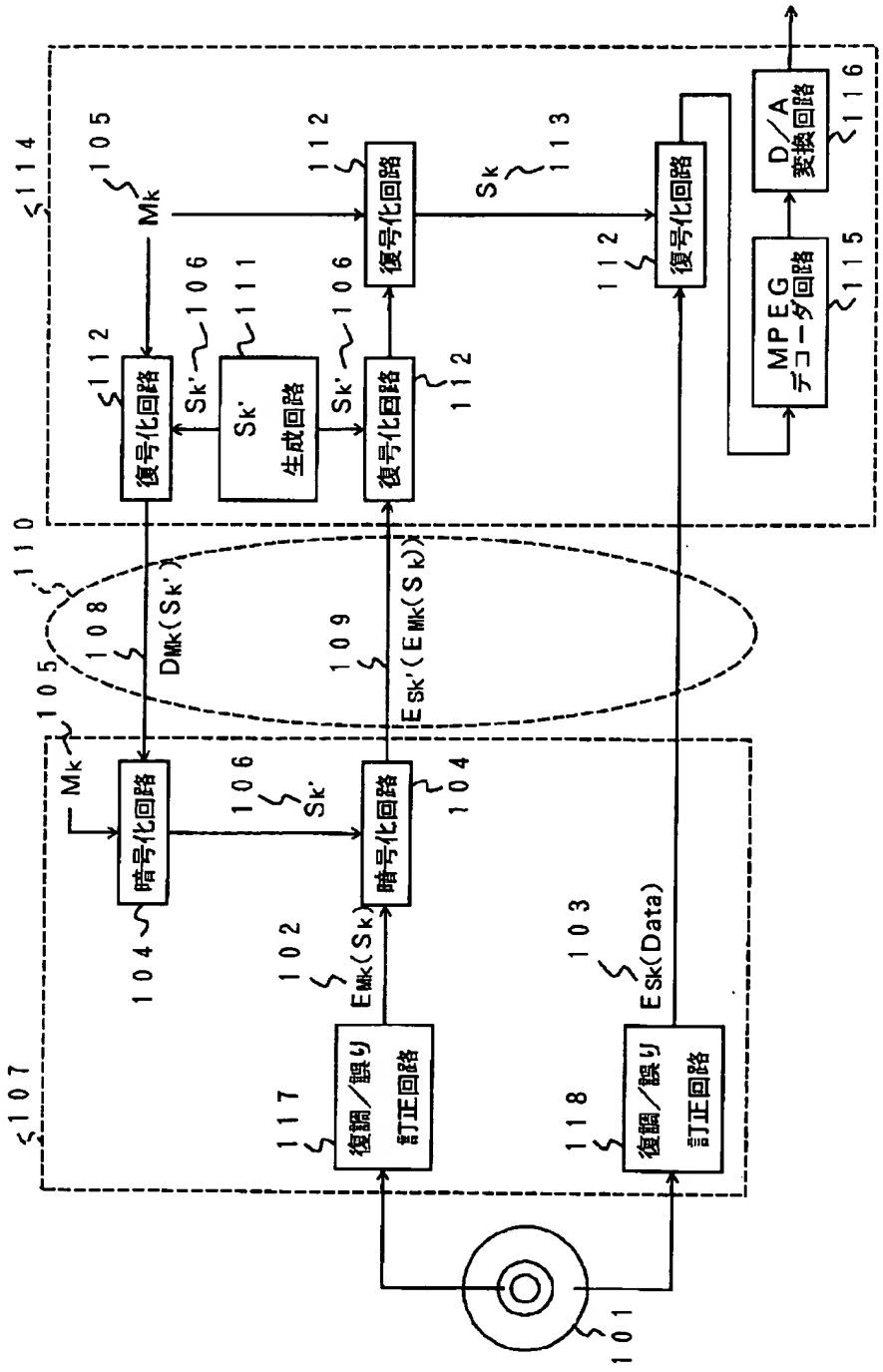
【図３】



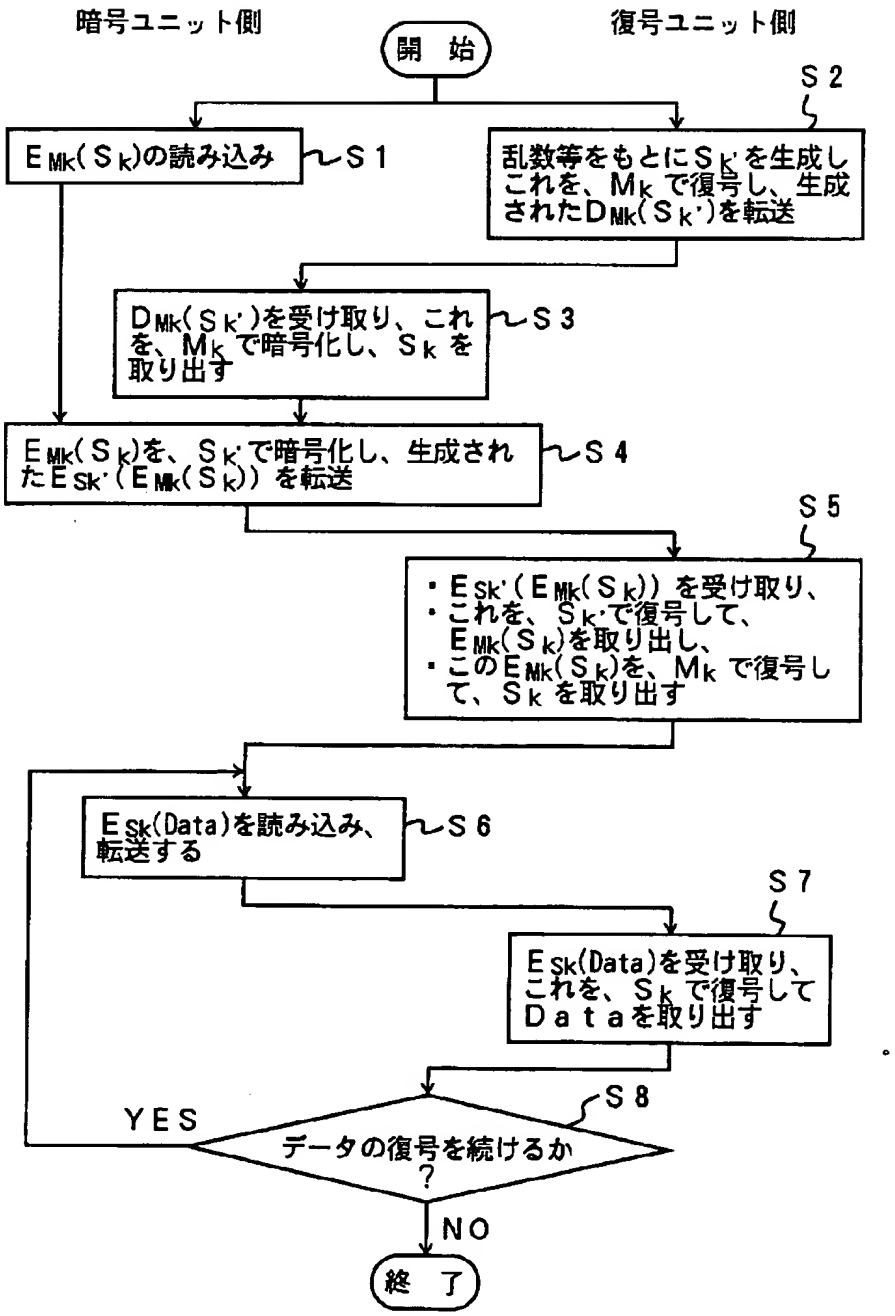
【図４】



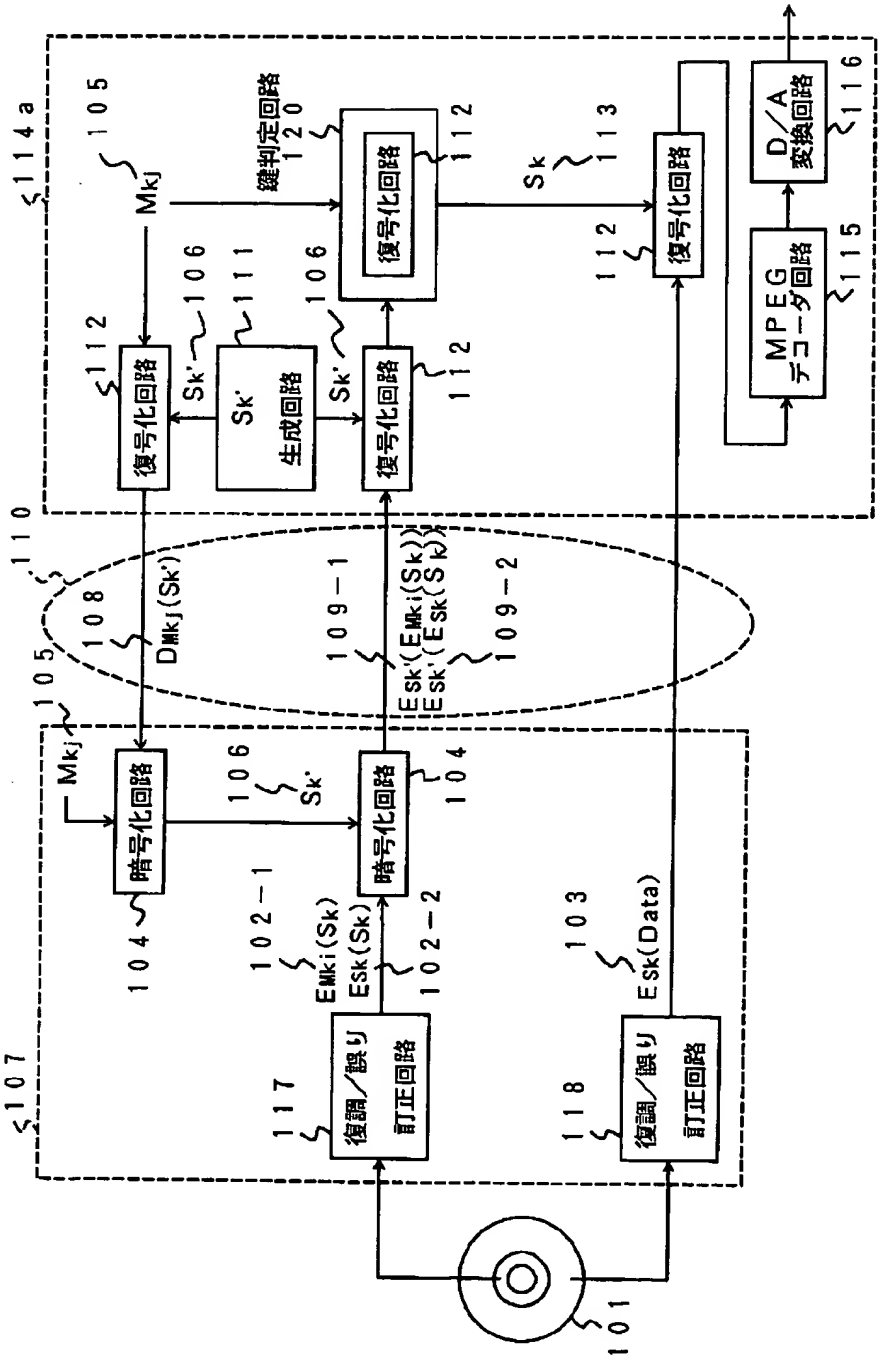
【図1】


114
105
Mk
112
復号化回路
Sk
113
D／A
変換回路
116
106
Sk'
111
Sk'
生成回路
106
Sk'
112
復号化回路
112
復号化回路
MPEG
デコーダ回路
115
110
108
Dmk(Sk')
109
Esk'(Emk(Sk))
105
Mk
暗号化回路
106
Sk'
104
暗号化回路
104
104
102
Emk(Sk)
103
Esk(Data)
107
117
復調／誤り
訂正回路
118
復調／誤り
訂正回路
101

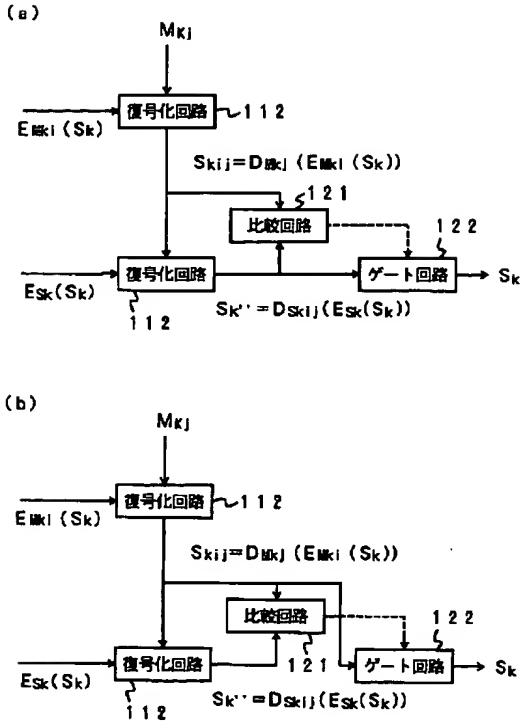
【図２】


暗号ユニット側
復号ユニット側
開　始
S２
$E_{Mk}(S_k)$の読み込み
S１
乱数等をもとに$S_{k'}$を生成しこれを、M_kで復号し、生成された$D_{Mk}(S_{k'})$を転送
$D_{Mk}(S_{k'})$を受け取り、これを、M_kで暗号化し、S_kを取り出す
S３
$E_{Mk}(S_k)$を、$S_{k'}$で暗号化し、生成された$E_{Sk'}(E_{Mk}(S_k))$を転送
S４
S５
・$E_{Sk'}(E_{Mk}(S_k))$を受け取り、
・これを、$S_{k'}$で復号して、$E_{Mk}(S_k)$を取り出し、
・この$E_{Mk}(S_k)$を、M_kで復号して、S_kを取り出す
E_{Sk}(Data)を読み込み、転送する
S６
S７
E_{Sk}(Data)を受け取り、これを、S_kで復号してＤａｔａを取り出す
S８
YES
データの復号を続けるか？
NO
終　了

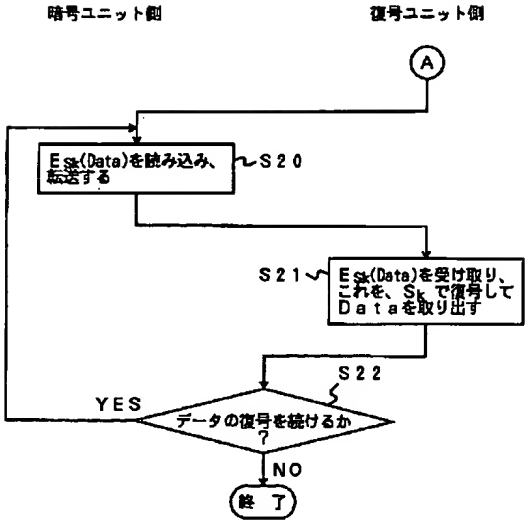
【図５】


１１４ａ
１０５
Mkj
鍵判定回路
１２０
復号化回路
１１２
Sk
１１３
D／A
変換回路
１１６
MPEG
デコーダ回路
１１５
１１２
復号化回路
１０６
Sk'
１１１
Sk'
生成回路
１０６
Sk'
１１２
復号化回路
１１０
１０８
DMkj(Sk')
１０９－１
ESk'(EMki(Sk))
ESk'(ESk(Skj))
１０９－２
１０５
Mkj
１０４
暗号化回路
１０６
Sk'
１０４
暗号化回路
１０２－１
EMki(Sk)
１０２－２
ESk(Sk)
１０３
ESk(Data)
１１７
復調／誤り
訂正回路
１１８
復調／誤り
訂正回路
１０７
１０１

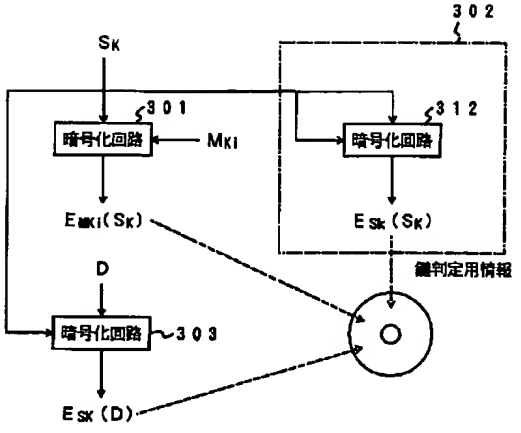
【図６】


(a)
MKJ
復号化回路
112
EMKI(SK)
SKIJ=DMKJ(EMKI(SK))
121
比較回路
122
復号化回路
ゲート回路
SK
ESK(SK)
112
SK''=DSKIJ(ESK(SK))
(b)
MKJ
復号化回路
112
EMKI(SK)
SKIJ=DMKJ(EMKI(SK))
比較回路
122
復号化回路
121
ゲート回路
SK
ESK(SK)
112
SK''=DSKIJ(ESK(SK))

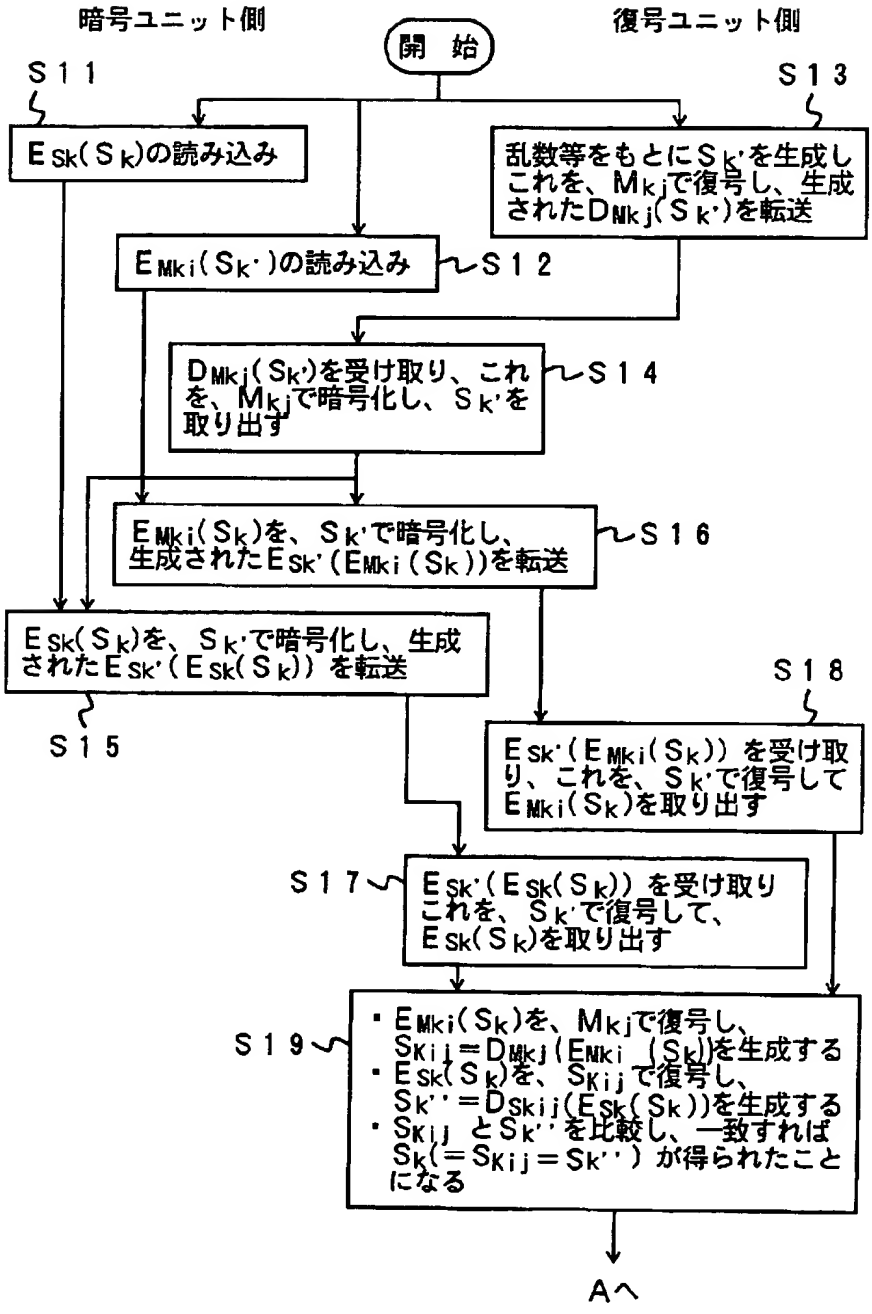
【図８】


暗号ユニット側
復号ユニット側
A
ESK(Data)を読み込み、転送する
S20
S21
ESK(Data)を受け取り、これを、SK で復号してDataを取り出す
S22
YES
データの復号を続けるか？
NO
終了

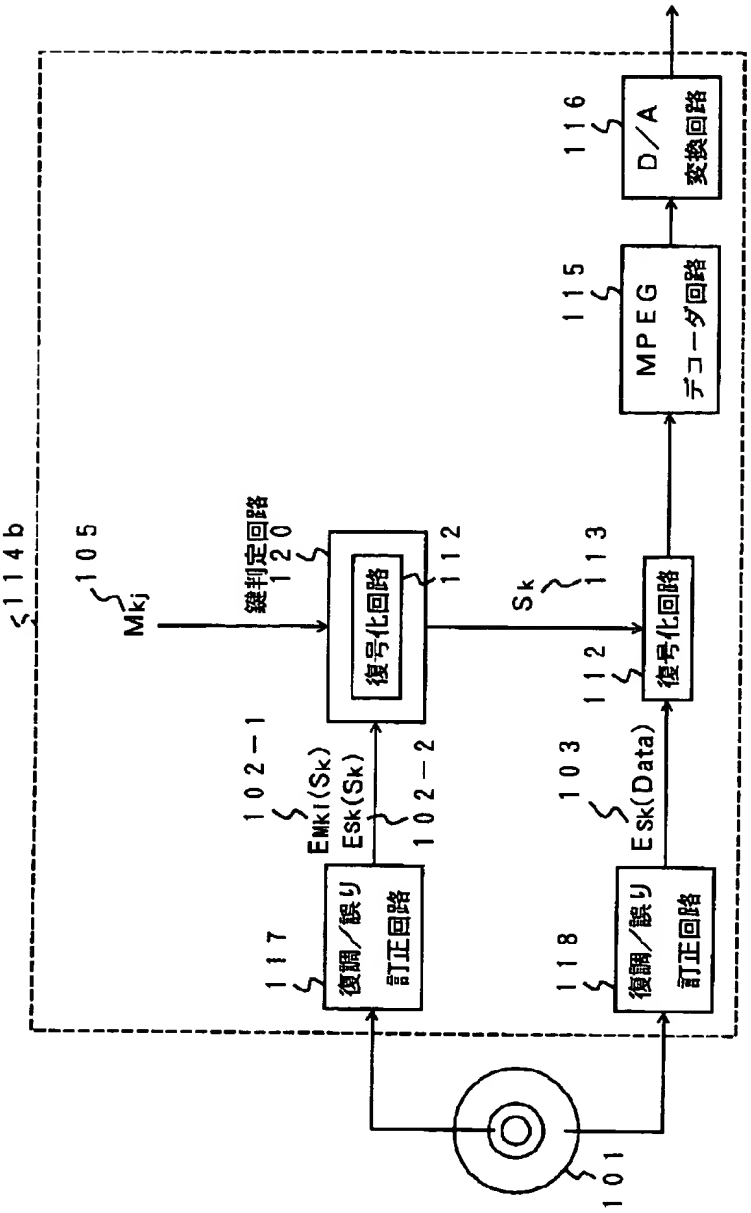
【図１２】


302
SK
301
312
暗号化回路
MKI
暗号化回路
EMKI(SK)
ESK(SK)
鍵判定用情報
D
暗号化回路
303
ESK(D)

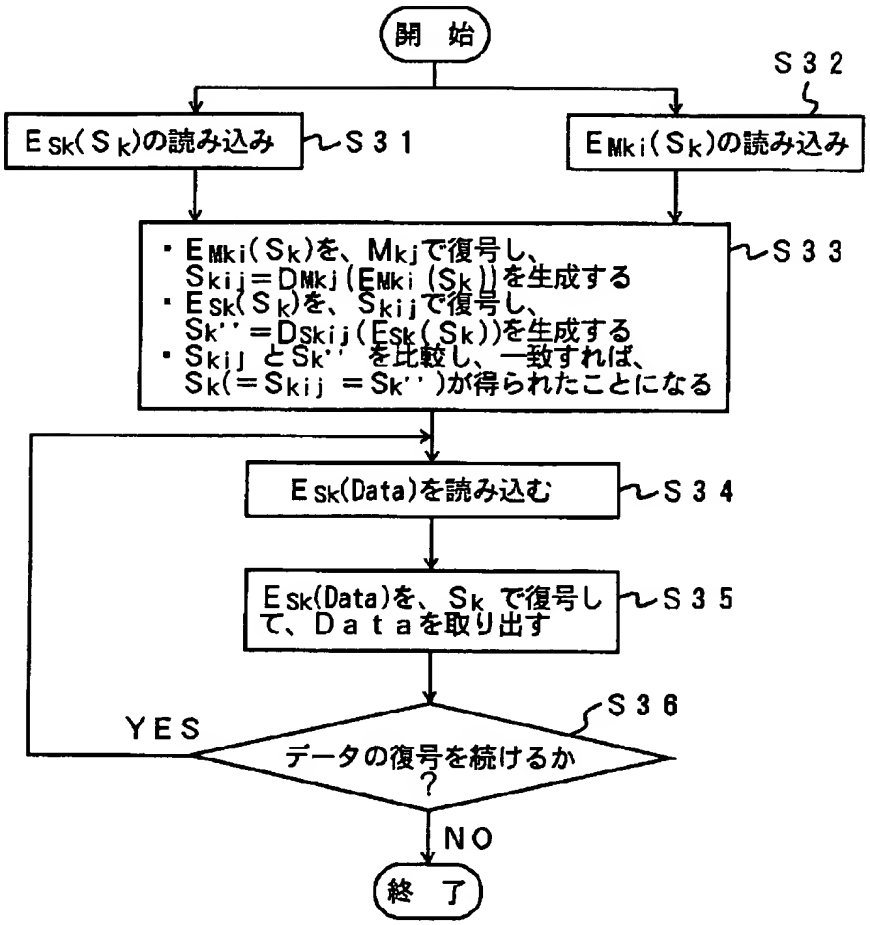
【図７】


暗号ユニット側
復号ユニット側
開　始
S１１
S１３
ESk(Sk)の読み込み
乱数等をもとにSk'を生成しこれを、Mkjで復号し、生成されたDMkj(Sk')を転送
EMki(Sk')の読み込み
S１２
DMkj(Sk')を受け取り、これを、Mkjで暗号化し、Sk'を取り出す
S１４
EMki(Sk)を、Sk'で暗号化し、生成されたESk'(EMki(Sk))を転送
S１６
ESk(Sk)を、Sk'で暗号化し、生成されたESk'(ESk(Sk))を転送
S１５
S１８
ESk'(EMki(Sk))を受け取り、これを、Sk'で復号してEMki(Sk)を取り出す
S１７
ESk'(ESk(Sk))を受け取りこれを、Sk'で復号して、ESk(Sk)を取り出す
S１９
・EMki(Sk)を、Mkjで復号し、SKij＝DMkj(EMki(Sk))を生成する
・ESk(Sk)を、SKijで復号し、Sk''＝DSkij(ESk(Sk))を生成する
・SKij とSk''を比較し、一致すればSk(＝SKij＝Sk'')が得られたことになる
Aへ

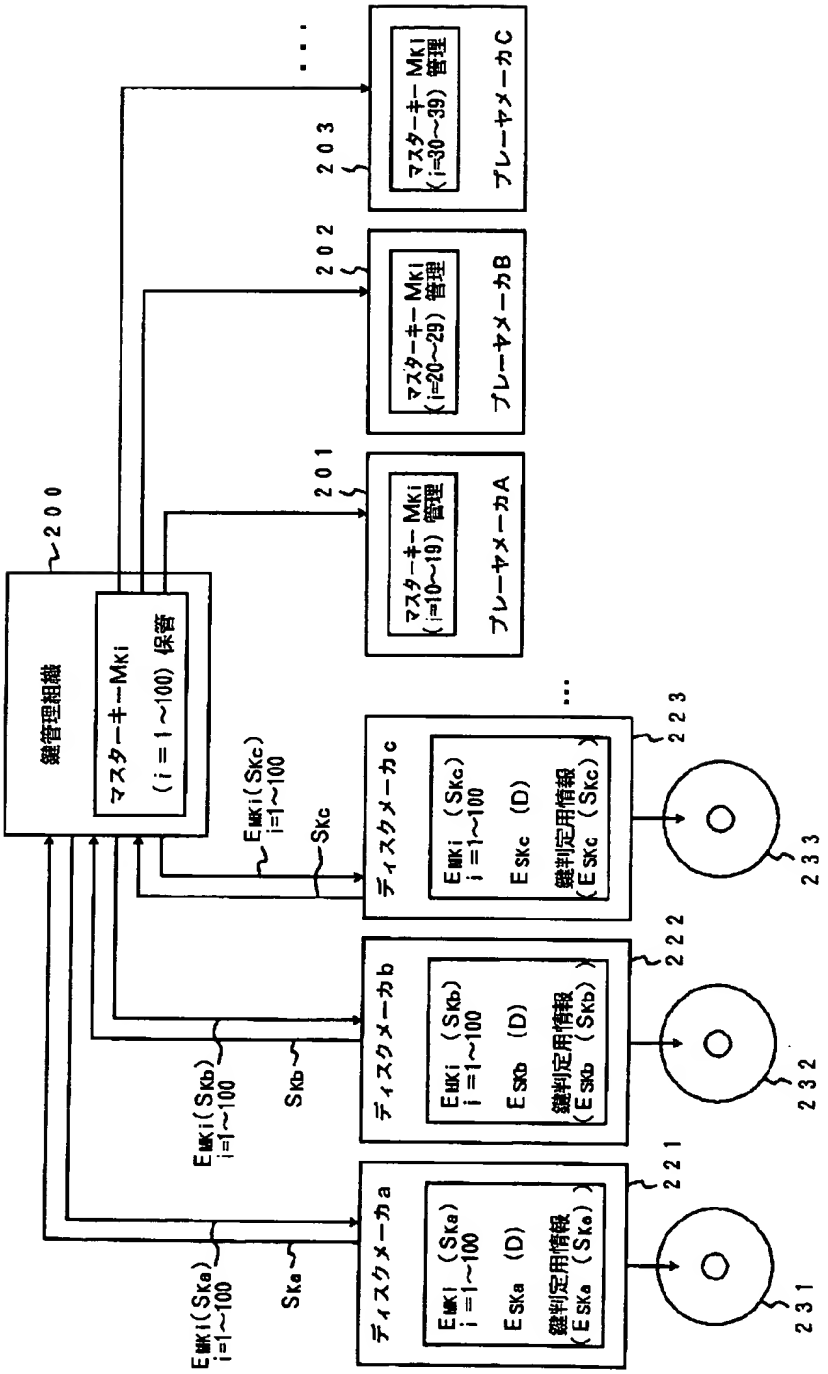
【図９】


114b
105
Mkj
鍵判定回路
120
復号化回路
112
Sk
113
復号化回路
112
102-1
EMki(Sk)
Esk(Sk)
102-2
103
Esk(Data)
117
復調／誤り訂正回路
118
復調／誤り訂正回路
115
MPEG デコーダ回路
116
D／A 変換回路
101

【図１０】


開　始
S３２
ESk(Sk)の読み込み
S３１
EMki(Sk)の読み込み
・EMki(Sk)を、Mkjで復号し、
Skij＝DMkj(EMki (Sk))を生成する
・ESk(Sk)を、Skijで復号し、
Sk''＝DSkij(ESk(Sk))を生成する
・Skij とSk'' を比較し、一致すれば、
Sk(＝Skij ＝Sk'')が得られたことになる
S３３
ESk(Data)を読み込む
S３４
ESk(Data)を、Sk で復号して、Ｄａｔａを取り出す
S３５
S３６
YES
データの復号を続けるか？
NO
終　了

【図１１】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI
		H04L 9/00　601E
		601B

(72)発明者　小島　正
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

(72)発明者　平山　康一
神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内